COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 1 décembre 2010 T-PD-BUR(2010)11

**LE BUREAU DU COMITE CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT AUTOMATISE DES DONNEES A CARACTERE PERSONNEL**

**(T-PD-BUR)**

22ème réunion
15-17 novembre 2010
Strasbourg, salle G04

# Etude sur la recommandation No. R (89) 2 sur la protection des données à caractère personnel utilisées à des fins d'emploi propositions de revision de la recommandtion ci-mentionnée

Par Giovanni Buttarelli

**Version Décembre 2010**



Document du Secrétariat preparé par
la Direction Générale des affaires juridiques et des droits de l'Homme

## TABLE DES MATIERES



## ANNEXE

## 1. LE NOUVEAU CONTEXTE DU MONDE DU TRAVAIL

L'étude menée sur la recommandation a été d'ordre général. Elle a fait référence à des problèmes d'application divers et nouveaux, tout en accordant une attention particulière aux technologies nouvelles et à leur influence sur le contrôle de l'activité des travailleurs. Le présent document tient compte de la demande qui a été faite de formuler des observations synthétiques.

Près de vingt-deux ans se sont écoulés depuis la recommandation. En termes de développement technologique, une si longue période équivaut à un siècle.

Au cours de cette période, le travail en tant que tel a beaucoup évolué (qu'il s'agisse de l'objet du travail, de la forme qu'il prend, de sa durée ou de ses acteurs intermédiaires), de même que les lieux sur lesquels il se déroule et son organisation. Les employeurs et les travailleurs ont changé, tout comme leurs besoins, et le nombre de données à caractère personnel enregistrées et traitées a augmenté (adresses IP, historiques et données de localisation par exemple). Ces facteurs ne sont pas seulement une conséquence du développement technologique.

Le travail a pris une nouvelle dimension internationale, étant à la fois d'envergure locale et globale, notamment en raison d'un important recours à la sous-traitance qui se pratique au niveau mondial (évoquons par exemple la délocalisation des centres d'appel). Les processus de production, bien qu'étant coordonnés de manière plus centralisée, sont parfois répartis sur de nombreux pays à l'échelle planétaire. Le *cloud computing* (informatique dématérialisée), c'est-à-dire le développement de technologies faisant appel à des ressources matérielles (stockage, CPU) ou logicielles situées à distance, fait partie des perspectives d'avenir relativement proches, ce qui ne simplifie pas les choses lorsqu'il s'agit de déterminer quelles lois s'appliquent au traitement des données.

L'osmose entre travail public et privé est plus étroite : le premier se distingue par un nombre croissant d'éléments contractuels caractéristiques du second. Dans le secteur public et dans certaines entités privées (comme les sociétés cotées en bourse), une plus grande transparence est exigée et est parfois garantie par la loi pour des raisons de maîtrise de la dépense, d'administration en ligne ou de bonne gouvernance d'entités publiques ou d'intérêt public. Cela accroît la nécessité de rendre publiques, y compris en ligne ou à la demande des personnes intéressées, des données à caractère personnel concernant les sélections par voie de concours, les coordonnées de contact de certaines personnes, le *curriculum vitae*, la fonction et la classe salariale. Il est donc plus nécessaire qu'auparavant d'expliquer en détail aux travailleurs quelles informations concernant leur relation de travail sont «publiques» ou, du moins, accessibles.

Au cours des dernières années, il a fallu tenir compte d'éléments nouveaux de même nature, notamment :

- à la suite de réglementations régissant les services financiers ;

- du chef de l'obligation légale pour les succursales établies dans certains pays (comme les États-Unis) de fournir des documents, des contenus et de nombreuses données à caractère personnel, y compris sur supports électroniques, concernant leurs employés et dirigeants, dans le cadre de litiges civils (*eDiscovery*) ou d'actions répressives, ce qui engendre parfois des conflits avec la protection des données dans d'autres pays ;

- en raison de l'identification de fraudes, dangers ou autres risques sérieux possibles susceptibles de nuire à des clients, à des collègues, à des actionnaires, au public ou à la réputation même de l'entreprise, de l'entité publique ou de la fondation (*whistleblowing*).

Indépendamment de la modernisation de l'organisation interne du travail, les données à caractère personnel traitées dans un but professionnel circulent beaucoup plus dans le monde entier et pas seulement au sein de succursales et de filiales. Les risques, responsabilités et incertitudes sont accrus quant à la possibilité que ces données puissent être plus facilement exploitées, après avoir été recueillies, à d'autres fins et dans d'autres conditions que celles initialement prévues ; ces données peuvent également être perdues, divulguées ou rendues accessibles à des tiers ou au sein du lieu de travail sans autorisation ni transparence.

Comme nous l'avons dit, en 22 ans les modalités de travail ont beaucoup évolué. S'il est vrai, par exemple, que le télétravail s'est répandu (bien qu'il ne soit pas utilisé de manière aussi intense que l'on avait pensée), il existe également de plus en plus de formes de travail fragmenté et temporaire, au service aussi de plusieurs employeurs, parfois dans le même cadre temporel ou par l'intermédiaire d'organisations qui opèrent en ligne.

Sur son lieu de travail physique principal (où se déroule la plus grande partie de son activité professionnelle), le travailleur est de plus en plus traçable à l'aide de divers dispositifs (accès aux systèmes informatiques et aux locaux ; appareils portables ; messageurs ; lecteurs RFID). Des éléments nouveaux importants pour la protection des données (pour la communication d'informations et en raison de l'utilisation de données d'une manière non transparente ou incompatible avec leur but originel) ont également été apportés par les systèmes électroniques de messagerie professionnelle, la téléphonie mobile et les téléphones intelligents, ainsi que certaines activités de travail spécifiques qui permettent de suivre en détail les déplacements de véhicules et de personnes notamment à l'aide de systèmes GPS (par exemple, les conducteurs de véhicules spéciaux ou le secteur du transport).

D'autres éléments nouveaux ont été générés par l'*ubiquous computing*, un nouveau modèle d'organisation *post*-desktop, qui implique un type différent d'interaction entre l'homme et la machine, par lequel l'élaboration des informations est intégrée au sein même des objets et des activités de tous les jours. Le travailleur utilisant l'*ubiquous computing* met en œuvre ou utilise, au cours de ses activités professionnelles habituelles, plusieurs systèmes ou appareils de traitement simultanément, et peut ne pas être conscient du fait que ceux-ci effectuent des opérations et collectent ou transmettent des données.

Par rapport au contexte de 1989, signalons également :

- dans le contexte de la protection des données, l'importance croissante de la réglementation sectorielle relative à la protection de la santé et de la sécurité physique des travailleurs. Nous évoquerons le rôle du «médecin compétent» sur un lieu de travail, qui doit mener de manière autonome un traitement des données relatives à la santé. L'employeur ne peut pas, en principe, accéder à ces données ; pourtant, il est coresponsable de la sécurité de leur traitement. Parfois, il est nécessaire également de traiter certaines données, pas toujours anonymes, concernant la population extérieure au lieu de travail (par exemple dans les entreprises menant des activités dangereuses) ;

- les conventions collectives ou les accords d'entreprise, ou les réglementations primaires ou secondaires, qui donnent aux organisations syndicales le pouvoir d'accéder à des données agrégées, anonymes ou parfois individuelles. De plus, les organisations syndicales utilisent *de facto*, ou avec l'accord de l'employeur, des systèmes informatiques internes du lieu de travail dans des buts d'information ou de prosélytisme, ce qui pose des problèmes ;

- la tendance des employeurs à collecter des données en dehors du cadre du travail, parfois même à l'insu des travailleurs, par exemple auprès des forces de l'ordre ou en ligne via les

moteurs de recherche et les réseaux sociaux, ce qui ouvre de nouvelles perspectives par rapport à ce qui a été analysé dans le *Memorandum* (point 11).

Tous ces nouveaux défis n'ont pas toujours fait l'objet d'une attention suffisante de la part des législateurs (y compris européen) et des autorités nationales de contrôle. Bien souvent, la protection des données dans le monde du travail demeure soumise aux mêmes principes que dans les autres secteurs publics et privés, le monde du travail ayant peu de règles spécifiques.

Les principes généraux des lois relatives à la protection des données demeurent valables et, du fait de leur caractère général, ils offrent une certaine flexibilité au monde du travail ; ils ne donnent cependant pas d'indications plus spécifiques, alors que cela serait parfois nécessaire (comme, par exemple, la nécessité d'interdire sur le lieu de travail toute discrimination fondée sur l'utilisation de données génétiques).

Plusieurs pays ont en revanche adopté de nouvelles lois de protection du travailleur, pour des raisons et dans des contextes différents de ceux des lois traditionnelles relatives à la protection des données. Celles-ci définissent des limites strictes, interdisant par exemple, en principe, la collecte de certaines données lors de la phase de recrutement, ou encore le recours à certaines questions ou certains tests d'aptitude, même si les personnes concernées sont éventuellement consentantes.

Dans ce domaine, les différences entre les approches des législateurs nationaux de chaque pays ne se sont que partiellement réduites. Aujourd'hui encore, des données de diverses catégories sont transmises à des bases de données centralisées auprès d'une «maison-mère», sur la base du consentement des personnes concernées, qui est, cependant, dans ce cas, peu approprié. Certaines entreprises utilisent, bien que de manière non systématique, des clauses contractuelles types régissant les rapports des *controllers* entre eux, ou entre *controllers* et *processors* ; ces clauses ont été élaborées, ou considérées adaptées, à la suite d'un intense débat qui s'est déroulé sur la scène européenne et internationale. Signalons également le développement progressif, bien que lent, de *codes of practice* (également dénommés *binding corporate rules*), grâce auxquelles les organisations multinationales concernées définissent des mesures internes pour couvrir les personnes concernées (audit, programmes de formation, réseau *privacy officers*, systèmes de traitement des plaintes, etc.), qui sont présentées comme «contraignantes» au sein du groupe d'entreprises puis validées par les autorités de protection des données.

## 2. LIGNES GENERALES POUR UNE MISE A JOUR DE LA RECOMMANDATION

Malgré ce contexte profondément modifié, ayant été rédigée selon une technique normative orientée vers le long terme, fondée sur des catégories de prescriptions générales et flexibles, la recommandation de 1989 demeure encore globalement valable, notamment compte tenu des garanties offertes par la «convention 108» et son protocole additionnel.

À ce jour, il est cependant légitime de maintenir une recommandation spécifique à ce sujet, après toutefois l'avoir mise à jour sur la base de certaines modifications visant non seulement à ajouter quelques éléments particuliers, mais également à développer les principes généraux actuellement en vigueur, dont l'efficacité semble valable pour les prochaines années.

Par souci de clarté, le texte organique d'une «nouvelle» recommandation, joint en annexe, met en évidence ces modifications et ajouts, tout en laissant la possibilité ouverte soit d'adopter une nouvelle recommandation qui remplacerait entièrement la précédente (bien qu'elle ne contiendrait, comme indiqué, que des modifications partielles et des ajouts : c'est la solution que nous

privilégions) soit d'approuver seulement chaque modification et ajout au texte de la recommandation actuelle, qui resterait donc formellement en vigueur.

Dans tous les cas, il convient de suivre une approche globale et de rester dans la ligne des autres recommandations du Conseil de l'Europe relatives à d'autres secteurs, certaines de celles-ci comprenant des indications utiles pour le monde du travail (notamment les recommandations R (86) relative à la protection des données à caractère personnel à des fins de sécurité sociale, R (95) relative à la protection des données à caractère personnel dans le domaine des services de télécommunications, et plus particulièrement des services téléphoniques, et R (97) relative à la protection des données médicales), laissant à d'autres entités le soin d'apporter d'éventuelles mises à jour limitées à chacun de ces instruments.

Par rapport au passé, le lieu de travail est aujourd'hui considéré comme une entité sociale où le travailleur a le droit de construire sa personnalité, et pas seulement par rapport à ses collègues au sein du lieu de travail, comme l'avait déjà souligné le *Memorandum*. D'importantes décisions jurisprudentielles reconnaissent au travailleur le droit de jouir d'une sphère privée raisonnable dans ses relations personnelles et professionnelles. Ce droit s'étend au-delà des espaces où les lois traditionnelles protègent déjà la vie privée (restaurants d'entreprise, armoires, tiroirs, vestiaires et, dans certaines limites, comportements individuels en dehors du lieu de travail). Les travailleurs peuvent ressentir le besoin, au cours de journées de travail parfois longues, d'utiliser l'internet pour de brèves interactions entièrement personnelles, par exemple pour le suivi d'un dossier administratif ou médical. Cela pourrait se faire selon des modalités et dans des limites acceptables par l'employeur et définies de manière transparente.

Il conviendrait de souligner dans le préambule qu'à l'échelle internationale apparaît un nouveau contexte, y compris en termes de jurisprudence, dont la tendance récente a été de défendre les libertés et les droits fondamentaux en matière de traitement des données, allant jusqu'à définir de nouveaux droits fondamentaux (par exemple le droit à la protection des données ou à l'inviolabilité du domicile virtuel), à reconnaître la dignité des travailleurs dans le contexte de la télésurveillance, ou encore à mieux garantir différentes formes d'*habeas corpus* ou d'*habeas data* dans le domaine de la biométrie et des données génétiques.

La recommandation devrait ne comprendre que des principes technologiquement neutres, capables de résister pendant quelques années au moins à un développement technologique qui s'annonce incessant, sans «suivre» des technologies ou des applications spécifiques qui devraient pourtant être mentionnées dans certaines parties du texte ou seulement dans le *Memorandum*.

Cependant, une recommandation en la matière ne devrait pas considérer les phénomènes évoqués plus haut du point de vue de l'automatisation, comme c'était le cas en 1989, cette perspective étant historiquement dépassée ; elle devrait plutôt prendre en compte la dimension virtuelle de nombreux lieux de travail. De plus, la recommandation actuelle accorde une attention toute particulière au moment de la «mise en place» des systèmes informatiques, plutôt qu'à leur fonctionnement, et ces considérations devraient être adaptées aux réalités d'aujourd'hui. L'utilisation des technologies et des systèmes informatiques est en effet, désormais, une habitude quotidienne. L'*e-workplace* est une réalité aussi variée qu'incontournable, qui demande plus d'attention aux nouvelles applications.

La recommandation devrait réglementer la relation traditionnelle de travail dans le secteur public comme dans le secteur privé, XXX sans distinction. Il serait par ailleurs utile de souligner que d'éventuelles adaptations de ses principes pourraient être nécessaires pour des situations spécifiques, en particulier dans le contexte des communications d'employés spécialement tenus de respecter le secret professionnel (comme c'est le cas, par exemple, des secrets industriels ou d'entreprise ou de la protection du secret des sources en matière de journalisme).

Il semble également utile d'accorder une plus grande attention à la diffusion croissante de données concernant des travailleurs à durée déterminée ou à temps partiel, dont les données peuvent être simultanément connues de plusieurs employeurs et intermédiaires, parfois par l'intermédiaire de systèmes en ligne utilisés à des fins d'assistance ou de sécurité sociale. Cette plus grande attention devrait également porter sur la durée de conservation des données relatives aux personnes qui ne sont pas embauchées, qui ne réussissent pas les tests d'aptitude ou qui effectuent un stage.

Il serait important de donner un signal clair dans le cadre de l'exercice du droit des personnes concernant les données d'évaluation. Un équilibrage raisonnable des intérêts en jeu pourrait permettre au travailleur d'accéder aux données le concernant à la fin du processus d'évaluation, tout en tenant compte de contraintes temporaires relatives à la protection de l'employeur ou de tiers ; en revanche, il ne devrait pas être possible de rectifier ces données, du moins selon les procédures traditionnelles de rectification.

En dernier lieu, le nouveau contexte des droits, à commencer par celui relatif à la protection des données à caractère personnel, fait apparaître le besoin d'une réflexion sur l'actuelle distinction entre traitements automatisés ou non. Il serait, de toute façon, utile d'apporter certaines précisions, bien que la recommandation interdise déjà toute possibilité de se soustraire aux dispositions en la matière (point 1.1).

## 3. ÉLEMENTS D'ELABORATION DE NOUVEAUX PRINCIPES ET LEURS DESTINATAIRES

Outre les modifications spécifiques portant sur des dispositions actuelles, qui seront indiquées en annexe, il semblerait opportun d'introduire dans la recommandation quelques indications qui s'inspireraient de cinq nouveaux principes, certaines d'entre elles pouvant s'avérer par ailleurs utiles à l'avenir pour des recommandations dans d'autres secteurs.

*Privacy by design*

La recommandation devrait rester principalement concentrée sur l'activité des responsables du traitement des traitements. Il serait cependant utile de s'intéresser aux acteurs concevant, produisant et distribuant des logiciels et des technologies (ainsi qu'aux chercheurs et organismes qui les certifient ou qui œuvrent à leur standardisation), de même qu'aux prestataires de services et aux fournisseurs d'accès. Une approche préventive, inspirée par la logique de *privacy by design*, pourrait réduire les problèmes d'application, favorisant la distribution de produits *privacy oriented*, plus respectueux, d'un point de vue technique et structurel, des principes de nécessité et de proportionnalité. Cela permettrait de limiter les retombées négatives résultant des processus de distribution et d'utilisation de ces produits.

*Accountability*

Il serait opportun d'insister sur *l'accountability* des responsables du traitement des données. Même dans le monde du travail, il est nécessaire de mieux traduire les principes généraux et les obligations légales en *best practices* concrètes, afin que la protection des données fasse, plus que par le passé, partie intégrante des valeurs partagées d'une organisation et qu'au sein de celle-ci, des responsabilités plus spécifiques soient définies. Il serait possible de parvenir à ce résultat en encourageant les responsables du traitement des données à adopter des mesures techniques et organisationnelles visant à respecter concrètement les obligations et principes susmentionnés, ce que le responsable du traitement des données devrait être capable de démontrer à la demande des autorités de surveillance.

Le *Memorandum* pourrait ensuite offrir quelques exemples de mécanismes efficaces, adaptés au cas par cas, en mesure de favoriser une véritable protection des données, tels que :

- des inventaires à jour des traitements ;

- des *binding internal procedures and/or policies*, préalables à l'introduction de nouvelles catégories de données ou de traitements, dont les obligations et le rôle seraient à adapter selon l'importance du cas ou de l'événement, par exemple pour préciser préalablement comment il convient d'informer les personnes concernées ou comment leur fournir une réponse adéquate s'ils souhaitent exercer leurs droits ou soumettre une plainte ;

- des *privacy impact assessments* pour les opérations de traitement comportant des risques majeurs ;

- la désignation d'un délégué à la protection des données, ou l'attribution de responsabilités plus spécifiques, afin de mettre en place une gestion des traitements plus organique ; l'introduction de mécanismes internes d'audit ou de vérification indépendante de l'état d'application de la loi ;

- l'identification de procédures internes pour signaler des violations ou des risques de sécurité ;

- des activités de formation à divers niveaux, y compris pour les cadres, ainsi que des certifications ;

Il conviendrait également de souligner que les mesures examinées n'alourdiraient pas les obligations des responsables du traitement des données et ne multiplieraient pas inutilement leurs obligations déjà existantes ; elles aideraient plutôt les responsables du traitement à garantir *de facto* une *compliance* effective et à mieux être en mesur de le démontrer en cas de contrôle ou de litige.

*Principe de nécessité*

En accord avec le principe de *privacy by design*, il serait utile de faire en sorte que les systèmes d'information et les programmes informatiques soient configurés de manière à réduire au minimum l'utilisation de données à caractère personnel et de données d'identification selon le but poursuivi. Il conviendrait par ailleurs de souligner le fait que l'employeur devrait traiter les données de la manière la moins invasive possible.

*Interdiction des traitements de données dans un but de télésurveillance*

Pour une meilleure protection de la dignité, il serait souhaitable de décourager plus explicitement les activités impliquant, même de manière discontinue, le traitement de données à caractère personnel visant *directement* et principalement à opérer une surveillance à distance (physique ou virtuelle) de l'activité professionnelle et d'autres activités personnelles. L'employeur devrait s'abstenir d'utiliser les résultats de tels traitements illicites, même si les travailleurs en ont été informés.

En revanche, les traitements qui n'impliquent une telle surveillance qu'*indirectement*, c'est-à-dire dont la finalité principale est liée à l'organisation ou à la sécurité professionnelle qui les rend nécessaires, pourraient être considérés licites ; mais ils devraient faire l'objet d'une information adéquate, mêmes aux organisations syndicales, sur la base, si possible, de leur accord.

*Principe de simplification pour les petites structures*

Enfin, il serait utile d'œuvrer vers une plus grande simplification des processus pour les petites structures professionnelles (petites entreprises, artisans, laboratoires), en proposant des ajustements dans l'application des règles de protection des données, afin d'éviter tout excès de démarches administratives, sans porter atteinte au niveau de protection.

**4. MISES A JOUR ET MODIFICATIONS SPECIFIQUES**

Compte tenu de la concision du texte demandé, ce document n'illustrera pas en principe les modifications mineures qui sont directement incluses dans le texte en annexe. En revanche, nous présenterons une synthèse de quelques thèmes sur lesquels il serait nécessaire de mettre à jour la recommandation ou le *Memorandum*. Comme nous l'avons dit, la recommandation est encore d'actualité en matière de réglementation générale sur certains sujets. Nous proposons, dès lors, d'insérer uniquement dans le *Memorandum* quelques éclaircissements, exemples, suggestions et précisions mentionnés dans le présent document, mais non insérés dans le texte en annexe.

*Collecte de données sur les réseaux sociaux*

Plusieurs employeurs (et intermédiaires) ont acquis une parfaite compréhension du fonctionnement des communautés virtuelles et d'autres services en ligne, parmi lesquels les réseaux sociaux (*Social Network Services*, ou SNS).

Les utilisateurs de ces plateformes de communication en ligne, qui connaissent une croissance exponentielle, y introduisent de nombreuses données et des contenus révélant des habitudes, des goûts, des relations d'amitié et des interactions avec d'autres utilisateurs, ce qui permet la création de profils structurés de personnes, basés sur leurs centres d'intérêt et activités.

L'accès à ces données peut être limité à des contacts choisis par l'utilisateur, mais certaines personnes ne limitent pas cet accès en acceptant systématiquement de nouveaux «contacts» sans se préoccuper des liens existants. Parfois, il est possible d'avoir accès aux contacts de tiers, même inconnus, par exemple lorsque toutes les personnes inscrites à un SNS peuvent consulter un profil, ou lorsque les données peuvent être indexées par des moteurs de recherche internes ou externes au SNS.

La modification des réglages par défaut, qui peuvent être défavorables à la protection de la vie privée, n'est effectuée que par une minorité des utilisateurs. Les données peuvent être utilisées par des tiers à diverses fins, y compris commerciales, et peuvent impliquer des risques tels que la perte d'opportunités commerciales et de possibilités d'emploi.

Alors que l'on a relevé plusieurs cas de licenciements motivés par un simple échange «privé» du travailleur, sur un SNS, de propos d'autodérision concernant ses conditions de travail, de nombreux utilisateurs continuent à revendiquer l'expectative légitime que les données à caractère personnel ayant été fournies dans le but de créer et d'entretenir des liens sociaux avec certaines personnes soient traitées de manière licite et correcte.

La recommandation devrait certainement tenir compte des obligations auxquelles sont déjà soumis les responsables du traitement des données au sein des SNS, spécialement en termes d'information, de *default*, et de proportionnalité. Cependant, il serait utile de fournir de brèves indications pour les cas où l'employeur, par le biais d'un intermédiaire, sous un autre nom ou en utilisant un pseudonyme, collecte et utilise des données relatives à des candidats à des prestations de services ou à des travailleurs, plus ou moins à leur insu, en les reliant parfois à d'autres informations. En principe, une telle collecte de données n'est en fait pas correcte, sans tenir compte du fait que le travailleur soit ou non inscrit au SNS (certains SNS permettent à leurs utilisateurs d'insérer des données [*tagging*]concernant des personnes non inscrites).

Il conviendrait de développer une approche différente pour les réseaux consacrés uniquement à l'échange de données professionnelles et relatives au travail, qu'il serait opportun de traiter de manière spécifique par rapport aux SNS plus «privés».

*Collecte de données par l'intermédiaire de moteurs de recherche ou et introduction de données d'employeurs en ligne*

Les réflexions évoquées plus haut pourraient également valoir pour la collecte périodique de données par l'intermédiaire de moteurs de recherche externes à l'organisation professionnelle.

Le problème de la «nature ouverte» de l'internet, ainsi que de la protection des données à caractère personnel de ses utilisateurs se pose également dans le cadre des procédures de sélection et des relations professionnelles.

Les moteurs de recherche font partie de la vie quotidienne des personnes qui utilisent l'internet et les nouvelles technologies pour trouver des informations. En tant que fournisseurs de services, ils collectent et traitent d'importantes quantités de données, celles-ci étant également collectées par des moyens particuliers comme les *cookies* (adresses IP, historiques de recherche, données fournies volontairement par l'utilisateur en vue de bénéficier de services personnalisés).

Les moteurs de recherche contribuent à faciliter l'accès à des informations aussi diverses que précieuses, offrant des possibilités sans cesse plus sophistiquées grâce à des services à valeur ajoutée tels que le profilage de personnes physiques (moteurs de recherche de personnes) et la reconnaissance faciale à partir d'images.

Ces outils donnent accès à de nombreux types de données, y compris des sons, des images, des vidéos et d'autres formats. Certains moteurs de recherche republient des données stockées dans une mémoire temporaire (mémoire cache). En regroupant des informations générales de différents types sur chaque individu, les moteurs de recherche sont en mesure de créer de nouveaux profils, peut-être inexacts, pour une personne ; celle-ci court donc un plus grand risque que si les données individuelles la concernant étaient consultées séparément.

La capacité des moteurs de recherche à regrouper des données peut avoir des effets significatifs sur la vie privée et la vie sociale de l'individu, surtout si les données personnelles présentées à l'issue d'une recherche sont incomplètes, excessives ou erronées, ou devraient être effacées en vertu du droit à l'oubli.

Malgré les progrès réalisés et les efforts fournis même par les autorités chargées de la protection des données, les utilisateurs n'ont pas encore suffisamment pris conscience des conséquences qui résultent de l'utilisation de ces services ni des objectifs, même secondaires, des opérations qui en découlent.

En théorie (même si ce n'est pas facile en pratique pour l'utilisateur moyen), le travailleur peut s'adresser au responsable d'un moteur de recherches pour faire effacer ou rendre anonymes les données à caractère personnel qui ne sont plus utiles pour la finalité pour laquelle elles ont été précédemment recueillies (en particulier lorsque les données ne correspondent plus au contenu effectif publié sur le site *web* «source»). Cependant, comme dans le cas des SNS, il y a lieu de prévoir l'exigence spécifique de faire en sorte que la collecte des données par les employeurs soit réalisée de manière pertinente et transparente.

Si la recommandation devait prendre en compte les moteurs de recherche, elle pourrait également tenir compte, dans un contexte tout autre de la problématique, du fait que les employeurs font une utilisation croissante de l'internet et de l'intranet afin de développer leurs propres sites web à des fins institutionnelles ou promotionnelles qui s'adressent aux citoyens, aux consommateurs et aux utilisateurs. De cette manière, une plus grande attention pourrait être accordée aux informations offertes aux travailleurs quant aux données les concernant qui sont destinées à être publiées, ainsi qu'au respect du principe de finalité.

*Données biométriques et technologie RFID*

La recommandation pourrait expressément tenir compte de l'utilisation croissante de systèmes biométriques, sans fil et de localisation, ainsi que de la technologie d'identification par radiofréquence (*Radio Frequency Identification*, plus connue sous le nom de «technologie RFID»), utilisés à des fins et dans des applications diverses, dont certaines sont susceptibles de violer la dignité humaine et les droits de la personne, ou d'exposer les utilisateurs à des risques majeurs.

L'employeur est en mesure de collecter, parfois de manière non transparente, différentes données relatives aux entrées, aux déplacements et aux activités des personnes, en particulier si celles-ci sont affectées à des travaux bien déterminés. Les données à caractère personnel relatives aux travailleurs sont également collectées de manière indirecte, par le biais du suivi d'objets et de produits dans le cadre du commerce de gros ou de détail et en traçant leurs déplacements.

L'utilisation de puces électroniques, souvent invisibles, présente des avantages pour l'employeur, puisqu'elle a des effets positifs sur l'organisation du travail et peut être facilement mise en place soit grâce à des appareils portables, soit en introduisant les puces dans des objets, des vêtements ou des uniformes, parfois avec le consentement (forcé) des personnes concernées, mais pas toujours dans le respect des principes de protection des données, principalement en raison de l'absence d'informations adéquates concernant l'utilisation des données. On peut même trouver des implants à introduire sous la peau du corps humain, qui se trouve ainsi changé en «antenne» ou récepteur, avec peu de considération pour l'*habeas corpus* et le principe (qui se trouve ici inversé) selon lequel les systèmes informatiques devraient être au service de l'homme.

Il conviendrait d'encourager l'adoption de règles internes en matière de confidentialité qui, tenant compte notamment du *Memorandum* explicatif, respectent plus spécifiquement les principes de :

- nécessité ;

- proportionnalité (y compris dans le contexte des différentes données biométriques, dont certaines sont plus délicates comme les empreintes digitales et la reconnaissance de l'iris, et d'autres moins invasives comme la physionomie de la main) ;

- finalité (exclusion de tout usage ultérieur, par exemple les données concernant les véhicules entrant dans les parcs de stationnement, qui peuvent être utilisées subrepticement pour les comparer avec les données de présence) ;

- information adéquate et intelligible y compris sur les types de données, sur le fait que les dispositifs recueillent des données sans que les intéressés adoptent consciemment un comportement actif, sur la possibilité - si elle existe - de désactiver et de réactiver les dispositifs ainsi que sur les conséquences qui en résultent, et enfin sur toutes les utilisations prévues des données ainsi que sur l'exercice du droit d'accès ;

- conservation limitée dans le temps des données.

L'utilisation raisonnable de ces systèmes devrait tenir compte du fait que certains choix comportent des effets plus ou moins invasifs: recours à des techniques de vérification et non d'identification ; création d'une base de données centralisée contenant des données biométriques, au lieu de n'inscrire ces données que dans un dispositif portable à la disposition des travailleurs ; utilisation de lecteurs plus puissants capables de lire les données à une plus grande distance ; adoption de solutions permettant ou non aux travailleurs de désactiver le dispositif.

En présence de garanties adéquates, le consentement des intéressés ne semble, cependant, du moins en principe, constituer le fondement idéal pour ces traitements.

*Unique identifiers*

Si des «identifiants uniques» sont utilisés sur le lieu de travail, il est plus facile de regrouper des données relatives à un travailleur et de créer des profils de manière peu visible. Cela peut être fait, par exemple, en distinguant les travailleurs selon des critères de qualité, de quantité et de durée des consultations de documents auxquels ils accèdent (par exemple dans les sociétés travaillant dans la production et la distribution de produits multimédia, désireuses d'éviter des violations du droit d'auteur par leurs travailleurs).

Ce sujet devrait être abordé de manière détaillée dans le cadre de la problématique du contrôle des travailleurs, tout en accordant une attention spécifique à l'éventuelle utilisation d'identifiants uniques, dans la mesure où ceux-ci permettent de révéler une volonté *a priori* de surveiller un travailleur. En principe, le *tagging* d'un document ne devrait pas être lié à un individu, à moins que cela soit indispensable pour mener à bien un service précis et que les utilisateurs en soient pleinement informés et, si possible, donnent leur accord.

*Données génétiques*

Certains employeurs ont manifesté un grand intérêt pour l'utilisation de données génétiques, en particulier avant l'embauche, dans le but de mieux approfondir le profil de candidats ou d'identifier ceux qui ne seraient pas adaptés à une certaine tâche (par exemple dans le cas d'une maladie déclarée ou d'un risque de maladie) ou pour identifier d'éventuelles mesures de protection visant à améliorer l'environnement de travail.

Cela implique également des risques possibles de discrimination et de graves violations de la dignité humaine, ainsi que du droit à l'autodétermination.

Les tests génétiques ont parfois une valeur incertaine en termes de prédictions et de probabilités, mais indépendamment de ces considérations, le traitement des données génétiques à des fins d'embauche devrait en principe être interdit et admis uniquement dans des circonstances exceptionnelles, en raison de finalités tout autres (notamment si un travailleur apporte lui-même des documents qui contiennent des données génétiques, confiés au praticien qualifié sur le lieu de travail en vue de faire adopter une mesure à son avantage ou pour le protéger, par exemple dans le cas d'une maladie professionnelle ou d'un litige).

*Données relatives à la séropositivité, au SIDA ou à l'abus de drogues ou d'alcool*

Une mise à jour ponctuelle du *Memorandum* pourrait être apportée sur le thème de la séropositivité et du SIDA, qui pose des problèmes analogues de discrimination éventuelle, mais implique également la nécessité de prendre des mesures de protection de la santé de tiers, par exemple des personnes que le travailleur assiste ou transporte. Plus spécifiquement, il pourrait être fait mention de la tendance raisonnable à identifier, de manière sélective, des situations ou des emplois exceptionnels susceptibles d'exposer réellement d'autres travailleurs ou des tiers à des risques sanitaires, qui devraient, dès lors, justifier une dérogation à l'interdiction tendancielle de traitement de ces données, moyennant des garanties appropriées y compris en ce qui concerne la diffusion des données collectées, la dignité et le droit de recours des personnes concernées.

*Accès aux dossiers médicaux conservés dans un autre lieu*

On note une utilisation croissante des dossiers médicaux électroniques, c'est-à-dire d'ensembles structurés de documentation médicale concernant l'état de santé physique et mental,

passé et présent, d'un individu ; ces dossiers permettent d'accéder rapidement à des données plutôt sensibles, en vue d'apporter des soins médicaux et à d'autres fins demeurant strictement dans le même cadre.

Les dossiers médicaux électroniques ne devraient être accessibles (outre au patient lui-même) qu'aux professionnels de la santé et au personnel autorisé des structures sanitaires qui interviennent dans les soins au travailleur, dotés en outre de droits de consultation «modulaires». La finalité principale de la consultation de ces dossiers devrait être de faciliter la réussite d'un traitement, grâce à de meilleures informations. L'accès aux dossiers à d'autres fins, y compris dans un but professionnel et même s'il a lieu par l'intermédiaire d'experts ou de compagnies d'assurances, devrait en principe demeurer interdit. Cette interdiction devrait s'appliquer tant à un éventuel accès direct en ligne par l'employeur (on commence à trouver sur le marché des dispositifs basés sur des jetons ou des signatures électroniques) qu'à un accès indirect par l'employeur qui peut faire pression sur le travailleur pour l'inciter à fournir des documents d'une manière qui n'est ni spontanée ni librement consentie.

Des garanties proportionnées devraient être prévues également pour les dossiers hors ligne.

## 5. LA SURVEILLANCE DES TRAVAILLEURS

*L'expectative raisonnable de droit à la vie privée sur le lieu de travail*

Les nouvelles technologies représentent également une évolution positive dans le monde du travail, bien que les employeurs puissent également les utiliser au détriment des libertés et des droits fondamentaux. Grâce à elles, il est plus facile d'analyser, de reconstruire et de dresser le profil de l'utilisation de systèmes d'information à des fins professionnelles, par exemple grâce aux historiques de navigation ou de connexion obtenus auprès de serveurs proxy ou d'autres instruments d'enregistrement des informations, qui permettent aussi à l'employeur de connaître le contenu des communications.

Le travailleur ne devrait pas laisser en dehors du lieu de travail ses propres droits au respect de la vie privée et à la protection des données. Au contraire, il devrait pouvoir s'attendre légitimement à un certain degré d'intimité y compris sur son lieu de travail, où se déroule une part importante de ses propres relations avec d'autres êtres humains. Cette attente ne devrait pas être compromise par le fait que le travailleur utilise des moyens de communication et des outils appartenant à son employeur.

La protection de la vie privée inclut le droit de mener des relations sociales, ce qui pose des limites aux prérogatives légitimes de l'employeur d'exercer une surveillance. L'employeur a le droit de promouvoir une gestion efficace et de se prémunir contre les responsabilités et les dommages que peuvent provoquer certaines actions des travailleurs. Les activités de contrôle et de surveillance menées dans l'intérêt de l'employeur devraient cependant demeurer licites, transparentes, efficaces et proportionnées ; cette approche raisonnable pourrait également prévenir une éventuelle dégradation de la qualité de la relation professionnelle.

La recommandation pourrait favoriser une approche commune dans ce domaine et un rapprochement des lois et des pratiques nationales, dans une perspective mondiale qui tiendrait compte du secret de la correspondance ainsi que des éventuelles dérogations susceptibles de s'y appliquer, ainsi que des pouvoirs d'information et de codécision exercés par les organismes de représentation des salariés sur la base de la loi ou de la convention collective.

Le concept moderne de «vie privée» comprend les activités de nature professionnelle ou commerciale. Le concept de secret de la correspondance s'est étendu également, puisqu'il s'est élargi au «secret des communications» de nouvelle génération.

L'emplacement et la propriété des moyens électroniques utilisés ne devraient pas fondamentalement lever le secret des communications et de la correspondance. La correspondance en ligne et la correspondance traditionnelle ne devraient pas être traitées différemment sans une raison valable : dans des conditions données, le courrier électronique devrait faire l'objet d'une approche analogue, bien que pas totalement identique, à celle adoptée pour le courrier traditionnel sur papier. Aujourd'hui déjà, et le phénomène n'ira que croissant au fil des années à venir, l'évolution des conditions de travail ne simplifie pas la séparation entre le temps de travail et la vie privée. En particulier, avec le développement du télétravail, de nombreux salariés continuent de travailler à domicile ou en dehors du bureau, utilisant des infrastructures informatiques mises ou non à leur disposition par leur employeur à cette fin.

Les réflexions menées dans le présent rapport concernent les situations les plus courantes auxquelles les travailleurs pourraient être exposés, mais il convient également de tenir compte des éléments suivants :

- des contrôles plus ou moins stricts pourraient être effectués pour des raisons autres que la sécurité ou la prévention et la détection de comportements illicites, par exemple en vue d'une surveillance de la productivité et de la qualité individuelle ou générale du travail ou d'une vérification du respect des heures de travail ;

- des contrôles généraux peuvent intéresser des cadres (administrateurs délégués ou chefs d'équipe), des professionnels autonomes exerçant sur leur lieu de travail (médecins), des personnes soumises à des contrôles internes effectués par une entité tierce (audits, conseils de surveillance), ou enfin des organisations syndicales. Toutes ces situations soulèvent des problèmes spécifiques, qui seront analysés séparément ;

- certaines activités professionnelles (transactions financières, formation professionnelle, p. ex. dans le domaine du marketing direct, des centres d'appels d'urgence) peuvent justifier, sous réserve de garanties adéquates, un enregistrement licite et honnête des contenus ou des données extérieures relatives aux communications ou aux conversations, à des fins de test ou d'étude ;

- des contrôles cachés par surprise peuvent être mis en place par l'employeur à la demande des autorités judiciaires ou policières, à des fins pénales et dans le respect de la législation.

Ces considérations portent sur le problème principal de la navigation sur l'internet et des messageries électroniques, ainsi que de l'utilisation d'appareils électroniques mis à la disposition du travailleur ; elles portent également, moyennant des adaptations appropriées, sur le thème plus classique des contrôles sur la téléphonie fixe sur les lieux de travail.

Le respect des règles de protection des données peut également prévenir d'autres problèmes concernant l'admissibilité des preuves lors des litiges civils, pénaux ou professionnels.

*Informations*

L'employeur devrait indiquer, dans tous les cas, de manière claire et détaillée, quelles sont les modalités d'utilisation permises des instruments mis à la disposition des travailleurs et si, dans quelle mesure et selon quelles modalités des contrôles sont effectués.

Les informations concernant la politique d'utilisation des moyens et les contrôles devraient être claires, complètes, précises et facilement accessibles.

Les informations devraient être adaptées à chaque contexte professionnel (par exemple aux petites structures, où les ressources d'information sont constamment partagées entre plusieurs personnes), faire appel à un langage clair, être publiées de manière accessible et mises à jour régulièrement.

L'employeur devrait par exemple préciser, selon les cas :

- les règles internes en matière de sécurité des données et des systèmes ou en matière de protection du secret d'entreprise ou professionnel prévues pour certaines catégories de travailleurs, ainsi que le rôle de l'administrateur du système et l'éventuelle délocalisation de serveurs dans d'autres pays ;

- les utilisations personnelles des instruments de communication électronique éventuellement permises, moyennant leur facturation à charge du travailleur, ou qui ne peuvent en aucun cas être tolérées (par exemple, le téléchargement ou la conservation de logiciels ou de fichiers n'ayant aucun rapport avec l'activité professionnelle), en indiquant également les conséquences possibles, de préférence adaptées à la gravité de l'infraction (il convient également de tenir compte de la possibilité d'une visite involontaire d'un site, résultant de manière imprévue de l'utilisation d'un moteur de recherche, d'une annonce publicitaire ou d'une erreur de frappe) ;

- les éventuels contrôles que l'employeur se réserve le droit d'effectuer, en indiquant leur raison légitime ainsi que leurs modalités de déroulement et les possibilités de recours des personnes concernées ;

- les catégories de fichiers d'historique éventuellement conservés, y compris au moyen de copies de sauvegarde, et les personnes ayant accès à ces fichiers.

Des informations similaires, mais pas nécessairement identiques, devraient être fournies, le cas échéant, aux organisations syndicales pouvant jouer un rôle en termes d'information, de consultation ou de concertation, notamment dans le cas de changements significatifs provoqués par l'introduction de nouvelles applications. Il y aurait lieu également d'étudier certaines formes de sensibilisation adaptée des personnes externes qui interagissent avec l'organisation, lorsque celles-ci sont concernées par l'activité de contrôle (par exemple, les destinataires de messages électroniques).

*Contrôles : nécessité et proportionnalité*

Dans la recommandation, ainsi que dans le *Memorandum*, il pourrait être indiqué qu'il incombe aux employeurs :

- d'assurer le fonctionnement et la bonne utilisation de moyens électroniques et de définir leurs modalités d'usage, tout en tenant compte de la réglementation relative aux droits et aux relations syndicales ;

- d'adopter des mesures de sécurité adéquates visant à assurer la disponibilité et l'intégrité des systèmes d'information et des données.

Sur la base d'objectifs déterminés, explicites et légitimes, l'employeur pourrait se réserver le droit de contrôler la qualité des prestations professionnelles de ses employés ainsi que leur bonne

utilisation des instruments de travail ou d'effectuer d'autres types de contrôle, par exemple en raison d'exigences de production, d'organisation ou de sécurité professionnelle (en cas d'anomalies ou pour les entretiens).

Comme indiqué plus haut, les activités ayant pour finalité principale la télésurveillance devraient être interdites, par exemple :

- l'enregistrement systématique, et l'éventuelle lecture, de messages électroniques ou de données extérieures relatives à ceux-ci, au-delà de ce qui est techniquement nécessaire pour le bon déroulement du service ;

- la mémorisation systématique des pages web visitées par les travailleurs ;

- l'analyse occulte d'ordinateurs portables confiés à des utilisateurs, par exemple au moment de leur entretien ou de leur remplacement ;

- la lecture et l'enregistrement occulte des caractères saisis à l'aide de claviers ou de périphériques analogues.

Le traitement des données relatives à un travailleur individuel devrait être autorisé lorsque cela est nécessaire à la poursuite d'intérêts légitimes de l'employeur (par exemple pour protéger l'organisation contre de sérieux risques de diffusion d'informations confidentielles) et ne contrevient pas de manière injustifiée aux droits fondamentaux des travailleurs.

La priorité devrait être donnée aux interventions préventives, y compris à l'aide de solutions d'ordre technologique.

Il convient d'interdire les contrôles effectués sans discrimination ou abusivement constants ou prolongés, qui ne peuvent par ailleurs trouver une facile justification dans le consentement du travailleur (dans une large mesure inapproprié, mais aussi insuffisant dans ce cas compte tenu de la présence de tiers).

Si l'employeur prévoit de procéder à des contrôles, il devrait en premier lieu vérifier que ceux-ci sont indispensables pour un but précis et sont proportionnés à l'objectif, tout en tenant compte d'autres moyens de surveillance moins invasifs en termes de vie privée (en évitant, par ,exemple le recours à des systèmes effectuant des contrôles automatiques et continus). Par ailleurs, divers logiciels sont capables de signaler automatiquement au travailleur qu'une certaine activité est illicite ou incorrecte, et ce type d'activité peut également être bloqué de manière automatique sans notification formelle du blocage éventuel.

La progressivité et la proportionnalité devraient également caractériser les cas où un manquement de la part du travailleur serait signalé à sa hiérarchie et à ses responsables (évaluation de la praticabilité d'avertissements à un niveau hiérarchique inférieur).

*Internet*

L'employeur, pour réduire le risque d'une utilisation inappropriée de l'internet (visite de sites non pertinents, téléchargement de fichiers ou de logiciels, utilisation de services non liés à l'activité professionnelle), devrait adopter les mesures qui conviennent, y compris des filtres, pour rendre inutiles des contrôles ultérieurs sur les travailleurs, susceptibles d'impliquer également des données sensibles. Ces mesures pourraient, par exemple, comprendre :

- l'identification et la définition a priori de catégories de sites n'ayant avec certitude aucun lien avec l'activité professionnelle ;

- la décision que les contrôles ne portent que sur des données anonymes ou empêchant l'identification immédiate des utilisateurs, grâce à une agrégation des données (par exemple, analyse d'historiques portant uniquement sur les connexions au web, pour des groupes de travailleurs).

L'employeur pourrait bien sûr ne pas laisser ses employés accéder à leur messagerie électronique ou à l'internet, mais dès lors qu'ils utilisent un ordinateur connecté au réseau, une interdiction absolue d'utiliser l'internet à des fins personnelles n'est pas compatible avec la réalité du monde du travail moderne.

Un éventuel abus de l'internet de la part des employés peut être détecté à l'aide de données agrégées ou anonymes, sans analyser le contenu des sites visités. Il peut suffire, pour vérifier que des abus n'ont pas lieu, de contrôler la durée de la navigation ou les catégories de sites les plus fréquemment visitées, même lorsque cette vérification porte sur la structure entière ou sur des départements spécifiques, et non sur des travailleurs individuels. S'agissant de ces derniers, des contrôles plus spécifiques pourraient être mis en place au cas où les premières vérifications d'ordre général mettraient en lumière d'éventuels abus.

*Courrier électronique*

Dans certaines situations, en particulier lorsque le lieu de travail n'est pas régi par une politique interne explicite et raisonnable, le contenu des messages électroniques - ainsi que certaines données extérieures à la communication et aux pièces jointes - pourrait faire l'objet d'une protection garantie par le secret de la correspondance et des communications, cette protection étant garantie également au niveau constitutionnel dans certains pays.

Le contrôle de la correspondance d'un travailleur ou de son utilisation de l'internet devrait n'être jugée nécessaire que dans des circonstances exceptionnelles.

Parfois, il peut tout simplement ne pas être facile de déterminer si un travailleur ayant envoyé ou reçu un message utilise la messagerie électronique à titre personnel ou s'il s'agit d'une communication professionnelle. Une politique interne adéquate permettrait donc d'éclaircir ce que les travailleurs et les personnes externes sont en droit d'attendre en termes de confidentialité, évitant ainsi que l'employeur ne se trouve dans une position illicite ou incorrecte lorsqu'il souhaite consulter le contenu des messages.

Afin d'empêcher les litiges fâcheux qui pourraient en résulter, l'employeur pourrait, par exemple :

- donner aux travailleurs le droit d'utiliser une autre adresse de messagerie électronique à usage privé, ou favoriser l'utilisation complémentaire d'adresses partagées entre plusieurs travailleurs au sein d'une seule unité ;

- faire en sorte qu'en cas d'absence du lieu de travail, le système informatique utilise une fonction communiquant automatiquement les coordonnées d'un autre point de contact utile ;

- mettre en place une procédure permettant, en cas de besoin, d'accéder de manière non conflictuelle, en cas d'absence du travailleur, à la messagerie électronique nécessaire au déroulement de l'activité professionnelle ; cet accès devrait s'inscrire dans une procédure transparente et correcte, qui devrait faire l'objet d'une information préalable auprès du travailleur, et qui lui permettrait de désigner au moment de la création du compte de messagerie une personne de confiance y ayant accès ;

- introduire dans certains messages électroniques un avertissement aux destinataires, indiquant la nature professionnelle des messages et la lecture possible du contenu des réponses.

Le contrôle de la messagerie électronique pourrait s'avérer nécessaire pour obtenir la confirmation ou la preuve que le travailleur a accompli certains actes illicites exigeant que l'employeur défende ses propres intérêts. C'est ainsi le cas lorsque l'employeur est subsidiairement responsable des actes commis par ses employés, lorsqu'il doit relever la présence de virus informatiques ou garantir la sécurité du système informatique ou encore lorsqu'il lui est indispensable d'accéder à la messagerie d'un employé en congé ou absent pour maladie.

Le contrôle de la messagerie électronique devrait en principe, au moins dans un premier temps, se limiter aux données concernant l'ensemble de la correspondance et la durée des communications, et non leur contenu, dans la mesure où ces données globales suffisent à dissiper les inquiétudes de l'employeur. L'accès au contenu de la messagerie électronique implique également d'autres personnes, au sein de la structure ou à l'extérieur, dont il n'est pas possible, en outre, d'obtenir le consentement.

Un contrôle anonyme infructueux pourrait être suivi d'un avis général aux travailleurs leur signalant qu'une utilisation incorrecte des instruments informatiques a été relevée, et les invitant à être plus attentifs aux instructions reçues.

Enfin, lors des éventuelles interventions de maintenance du système informatique, il devrait en principe être interdit d'accéder aux données personnelles stockées dans des dossiers ou dans des espaces de mémoire destinés aux travailleurs.

*Conservation des données*

En vertu du principe de nécessité, les logiciels devraient être programmés de manière à effacer régulièrement et automatiquement les données à caractère personnel concernant l'accès à l'internet et les télécommunications (par exemple en écrasant les données précédemment enregistrées). En l'absence d'exigences particulières liées à des aspects techniques ou de sécurité, la conservation temporaire des données relatives à l'utilisation des instruments électroniques devrait être justifiée par une finalité concrète, limitée à une durée nécessaire et prédéterminée. Un prolongement exceptionnel de la durée de conservation ne devrait avoir lieu que pour des raisons tout à fait spécifiques d'ordre technique ou liées à la sécurité, ou à des fins juridiques ou de défense.

Conformément au principe de proportionnalité, l'employeur ne devrait pas conserver les données obtenues à la suite d'une activité de contrôle pendant plus longtemps que nécessaire aux fins déclarées, exception faite d'exigences légitimes de défense ou juridiques. Les données ne devraient pas être exploitées à d'autres fins.

## 6. LA VIDEOSURVEILLANCE

Environ huit ans après leur adoption, les *«Guiding Principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance»* (principes directeurs pour la protection des personnes physiques à l'égard de la collecte et du traitement des données au moyen de la vidéosurveillance), adoptés par le Comité européen de coopération juridique lors de la 78e réunion du 20 au 23 mai 2003, demeurent d'actualité et ne semblent pas exiger un développement spécifique de la recommandation dans le cadre de la relation de travail.

Pour éviter de surcharger la recommandation et d'y apporter des modifications trop générales ou trop spécifiques à la sous-thématique de la vidéosurveillance, nous suggérons de ne pas introduire de nouvelles dispositions concernant cette question et d'y faire un simple renvoi soit dans le préambule, soit de manière plus diffuse dans le *Memorandum*, ce qui permettrait d'offrir une vision homogène de ces questions. Un renvoi similaire dans le préambule a été effectué par la recommandation de l'Assemblée parlementaire de 2008 concernant la vidéosurveillance dans les lieux publics.

## 7. CONCLUSION

Près de vingt-deux ans se sont écoulés depuis son adoption, mais le texte de la recommandation R (89) 2 demeure d'actualité à plusieurs titres, notamment en raison de l'approche orientée vers le long terme pour ses principes généraux employée lors de sa rédaction.

Des changements significatifs sont cependant intervenus dans l'organisation du travail, notamment en raison du développement des nouvelles technologies, des moteurs de recherche, des réseaux sociaux et des données biométriques, qui contribuent à créer un contexte très différent.

Il serait donc utile d'introduire dans la recommandation ou dans le *Memorandum* quelques indications s'inspirant de récents principes généraux qui se sont développés dans le cadre de l'évolution technologique, d'une manière technologiquement neutre (*privacy by design*, *accountability*, nécessité, interdiction des traitements de données ayant pour objectif principal la télésurveillance, simplification).

Dans le cas précis du contrôle de l'activité des travailleurs, quelques autres modifications et ajouts seraient utiles, et dans certains cas uniquement au *Memorandum*, tout en veillant, pour plus de commodité lors de son interprétation, à remplacer intégralement la recommandation.

Nécessité, proportionnalité et transparence sont des principes capables de contribuer à prévenir d'éventuelles tensions sur le lieu de travail, en instaurant un équilibre entre la nécessité pour l'employeur de contrôler que ses instruments électroniques sont correctement utilisés et le désir légitime de l'employé de jouir d'un certain degré de protection de sa vie privée et de pouvoir s'épanouir sur son lieu de travail.

**ANNEXE 1 : PROJET DE RECOMMENDATION CM/REC(2010)… DU COMITE DES MINISTRES AUX ETATS MEMBRES SUR LA PROTECTION DES DONNEES A CARACTERE PERSONNEL UTILISEES A DES FINS D'EMPLOI.**

*(Adopté le … 2010 par le Comité des Ministres*
*lors de la … réunion des Ministres délégués)*

Le Comité des Ministres, en vertu de l'article 15.b du Statut du Conseil de l'Europe,

Considérant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres ;

Conscient de l'utilisation croissante **des nouvelles technologies et des instruments de communication électronique** dans les relations entre employeurs et employés et des avantages qui en découlent ;

Estimant, toutefois, que l'utilisation **de méthodes de traitement informatique des données, notamment automatisé**, par les employeurs devrait être gouvernée par des principes destinés à réduire au minimum les risques que de telles méthodes pourraient éventuellement présenter pour les droits et les libertés fondamentales des employés, notamment leur droit au respect de la vie privée **et à la protection des données à caractère personnel** ;

Ayant à l'esprit les dispositions de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981, **ainsi que celles du Protocole additionnel concernant les autorités de contrôle et les flux transfrontières de données du 8 novembre 2001**, et compte tenu de la nécessité d'adapter ces dispositions aux exigences propres au secteur de l'emploi ;

Reconnaissant également que, lors de l'élaboration de principes dans le secteur de l'emploi, il doit être tenu compte aussi bien des intérêts individuels que des intérêts collectifs ;

Conscient des traditions différentes existant dans les Etats membres en ce qui concerne la réglementation des divers aspects des relations employeur-employé, la réglementation par voie législative ne constituant qu'une des méthodes utilisées ;

Rappelant dans ce contexte l'article 6 de la Charte sociale européenne du 18 octobre 1961,

**Conscient que les changements survenus dans la dimension internationale du travail dans le secteur public et privé, dans les processus de production et dans leur mondialisation favorisée par des technologies innovantes qui feront l'objet de développements futurs et intenses, imposent la révision de certaines dispositions de la Recommandation N° R (89) 2 sur la protection des données à caractère personnel utilisées à des fins d'emploi ;**

**Étant donné qu'il n'est pas nécessaire d'introduire, aux termes de ladite nouvelle Recommandation, d'autres principes spécifiques concernant l'utilisation d'instruments de vidéosurveillance, dès lors que les «Guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance adopted by the Council of Europe's European Committee on Legal Co-operation (CDCJ) in May 2003», rappelés dans la Résolution 1604 (2008) de l'Assemblée parlementaire du Conseil de l'Europe, demeurent valides ;**

Rappelant, dans ce contexte, l'article 6 de la Charte sociale européenne du 18 octobre 1961 **et le Code de conduite du Bureau international du travail de 1997 sur la protection des données à caractère personnel**,

Recommande aux gouvernements des Etats membres :

- d'assurer que les principes contenus dans la présente recommandation soient reflétés dans la mise en oeuvre des législations nationales relatives à la protection des données dans le secteur de l'emploi, ainsi que dans d'autres branches du droit portant sur l'utilisation de données à caractère personnel à des fins d'emploi ;

- d'assurer, à cette fin, que la recommandation soit portée à l'attention des autorités établies conformément à la législation nationale en matière de protection des données et chargées de contrôler l'application de cette législation ;

- de promouvoir l'acceptation et l'application des principes contenus dans la présente recommandation en assurant une large diffusion de celle-ci auprès des organes représentatifs des employeurs et des employés ;

**Décide que la présente recommandation remplace la Recommandation N° R (89) 2 sur la protection des données à caractère personnel utilisées à des fins d'emploi.**

**Annexe à la Recommandation**

1. *Champ d'application et définitions*

1.1. Les principes de la présente recommandation s'appliquent à la collecte et à l'utilisation de données à caractère personnel à des fins d'emploi dans les secteurs public et privé.

Ces principes s'appliquent aux données traitées automatiquement ainsi qu'aux autres informations sur les employés détenues par les employeurs dans la mesure où ces informations sont nécessaires pour rendre intelligibles les données traitées **automatiquement ou utilisées pour prendre d'importantes décisions. De même, ces principes s'appliquent, s'il y a lieu, aux données à caractère personnel relatives à des personnes extérieures au lieu de travail traitées à des fins de sécurité du travail, ainsi qu'aux organisations syndicales**.

Un traitement de données ne devrait pas être effectué par voie manuelle par un employeur dans le but d'échapper aux dispositions de la présente recommandation.

1.2. Nonobstant le principe énoncé au deuxième alinéa du paragraphe 1.1, un Etat membre peut étendre les principes énoncés dans la présente recommandation à tous les traitements manuels.

1.3. Aux fins de la présente recommandation :

– L'expression «données à caractère personnel» signifie toute information concernant une personne physique identifiée ou identifiable. Une personne physique n'est pas considérée comme identifiable si cette identification nécessite des délais, des coûts et des activités déraisonnables.

– L'expression «à des fins d'emploi» concerne les rapports entre employés et employeurs relatifs au recrutement des employés, à l'exécution du contrat de travail, à la gestion, y compris les obligations découlant de la loi ou de conventions collectives, ainsi que la planification et l'organisation du travail.

1.4. Sauf législations nationales contraires, les principes de la présente recommandation s'appliquent, dans les cas appropriés, aux activités des agences pour l'emploi, dans les secteurs public et privé, qui collectent et utilisent, **notamment par l'intermédiaire de systèmes d'information en ligne**, des données à caractère personnel afin de permettre l'établissement **d'un ou de plusieurs contrats de travail contemporains ou à temps partiel** entre les personnes qui figurent sur leurs listes et d'éventuels employeurs, **ou afin de faciliter les démarches dérivant desdits contrats**.

1.5. La présente recommandation ne s'applique pas, dans la mesure nécessaire à la protection de la sécurité de l'Etat, de la sûreté publique et de la répression des infractions pénales, aux informations confidentielles collectées ou détenues par l'employeur à des fins d'emploi sur des personnes recrutées pour un emploi ou exerçant un emploi en relation étroite avec ces domaines.

2. *Respect de la vie privée, de la dignité humaine* ***et de la protection des données à caractère personnel***

Le respect de la vie privée et de la dignité humaine **et la protection des données à caractère personnel, notamment relativement à la possibilité pour les employés de développer leur personnalité** dans les relations sociales et individuelles sur leur lieu de travail, devraient être préservés lors de la collecte et de l'utilisation de données à caractère personnel à des fins d'emploi.

**3.** ***Nécessité, développement de certains principes et simplifications***

**3.1. Les systèmes d'information, les programmes informatiques et les dispositifs électroniques utilisés à des fins d'emploi devraient être configurés, le cas échéant certifiés, et, en tout état de cause, devraient s'adapter à chaque lieu de travail afin de réduire au minimum l'utilisation et la conservation des données à caractère personnel, ainsi que de données permettant une identification directe, qui ne sont pas nécessaires pour atteindre les objectifs propres à chaque situation.**

**3.2. L'employeur devrait développer des mesures efficaces visant à garantir que les principes et les obligations en matière de traitement des données aux fins d'emploi soient réellement respectés, et pour pouvoir le prouver de manière adéquate sur demande des autorités de contrôle.**

**3.3. Les petites entreprises devraient adopter des solutions simplifiées adaptées.**

4. *Information et consultation des employés*

**4.1. L'installation et l'utilisation de systèmes d'information, de programmes informatiques et de dispositifs électroniques utilisés directement et essentiellement afin de contrôler à distance le travail, le comportement ou la position des employés, ne devraient, en principe, pas être autorisées.**

4.2. Conformément aux législations et pratiques nationales et, le cas échéant, aux conventions collectives, les employeurs devraient informer ou consulter leurs employés ou les représentants de ceux-ci préalablement à l'introduction, à la modification **et au fonctionnement** de systèmes

**d'information, de programmes informatiques et de dispositifs électroniques** pour la collecte et **l'utilisation des données à caractère personnel nécessaires aux fins de la production, de la sécurité ou de l'organisation du travail**.

4.3. **L'employeur devrait adopter des mesures appropriées pour évaluer l'impact d'éventuels traitements de données qui menacent précisément le droit au respect de la vie privée, la dignité humaine et la protection des données à caractère personnel, et pour traiter ces données de la façon la moins invasive possible**. L'accord des employés ou de leurs représentants devrait être recherché avant l'introduction ou la modification de tels systèmes, **programmes** ou dispositifs lorsque la procédure de consultation mentionnée au paragraphe 4.2 révèle **ce type de menace,** à moins que d'autres garanties appropriées ne soient prévues par la législation ou la pratique nationales.

5. *Collecte des **données et formes particulières de traitement ou d'informations***

5.1. Les données à caractère personnel devraient en principe être recueillies auprès de **l'intéressé**. Lorsqu'il convient de consulter des sources en dehors des contrats de travail, **ce dernier** devrait en être informé.

5.2. Les données à caractère personnel collectées par les employeurs à des fins d'emploi devraient être pertinentes et non excessives, compte tenu du type d'emploi ainsi que des besoins évolutifs d'information de l'employeur.

5.3. Au cours d'une procédure de recrutement **ou d'avancement** des employés, les données collectées auprès des candidats devraient se limiter à celles qui sont nécessaires pour évaluer l'aptitude des **intéressés** et leurs perspectives de carrière.

Au cours d'une telle procédure, les données à caractère personnel devraient être recueillies uniquement auprès de l'individu concerné. Sous réserve des dispositions du droit interne, d'autres sources, **dont celles en provenance de sociétés de conseil ou de réseaux sociaux dédiés au développement de relations professionnelles**, ne peuvent être consultées que si la personne concernée y a consenti ou si elle a été informée au préalable de cette possibilité. **Le profilage de l'intéressé basé sur la collecte occulte de données provenant de moteurs de recherche devrait être, en principe, interdit. L'employeur ne devrait pas inciter l'intéressé à lui fournir un accès à son dossier électronique de sécurité sociale conservé par des tiers.**

**Il conviendrait, en tout état de cause, de prendre des mesures appropriées afin que, parmi les données facilement accessibles sur des réseaux de communication électronique à disposition du public, seules les données pertinentes, exactes et mises à jour soient utilisées, ce qui éviterait que ces données soient mal interprétées ou traitées de façon déloyale en raison de leur provenance.**

5.4. Le recours à des tests, à des analyses et à des procédures analogues destinés à évaluer le caractère ou la personnalité d'une personne ne devrait pas se faire sans son consentement, ou à moins que d'autres garanties appropriées ne soient prévues par le droit interne. La personne concernée devrait pouvoir, si elle le désire, connaître **au préalable les modalités d'utilisation** des résultats de ces tests, **les analyses ou les procédures et, par la suite, leur contenu.**

**5.5. Le traitement des données biométriques visant à identifier ou authentifier les personnes devrait se fonder sur des méthodes scientifiquement reconnues. En principe, le traitement de ces données ne devrait être permis que lorsqu'il est nécessaire à la protection des intérêts primordiaux de l'employeur ou pour protéger l'intégrité personnelle et la santé des employés ou de tiers.**

**5.6.** **Eu égard à l'éventuel traitement de données à caractère personnel figurant sur des pages du réseau Internet ou Intranet consultées par l'employé, il conviendrait d'adopter, sous réserve d'en informer les intéressés conformément aux paragraphes 4 et 12, les mesures préventives suivantes :**

**la configuration de systèmes ou l'utilisation de filtres qui permettent d'empêcher, selon le cas, certaines opérations (comme téléverser ou télécharger des contenus précis) ;**

**l'identification de catégories de sites jugés comme corrélés ou non au travail de l'employé ;**

**la graduation des éventuels contrôles relatifs aux données à caractère personnel, moyennant dans un premier temps des contrôles par sondages non individuels sur des données anonymes ou groupées (par exemple, par unité de production).**

**Si l'employé utilise, conformément à l'autorisation donnée par son employeur, des biens susceptibles de signaler l'endroit où il se trouve en dehors de ses heures de travail, il conviendrait d'adopter des mesures permettant d'empêcher que ces données soient utilisées et de les effacer automatiquement le plus vite possible.**

**Il conviendrait de définir des procédures internes relatives au traitement de ces données en les portant préalablement à la connaissance des intéressés.**

**5.7.** **Sans préjudice des dispositions du paragraphe 4, point 1, l'employeur devrait, en principe, s'abstenir de consulter systématiquement le contenu des messages de courrier électronique adressés à ou envoyés par un employé possédant une boîte de courrier électronique identifiée.**

**Si possible, il serait préférable d'attribuer aux employés des adresses de courrier électronique qui ne fassent pas référence immédiatement à des personnes mais à des fonctions.**

**Il conviendrait également de fournir des instructions afin que, en l'absence d'un employé, le système de messagerie électronique signale l'absence temporaire de l'employé et communique automatiquement les coordonnées d'un autre contact utile. Pour des situations exceptionnelles, en cas d'absence d'un employé, une procédure ad hoc devrait contrôler uniquement l'ouverture des messages électroniques qui concernent le travail, si possible en prévenant l'employé en question, et, le cas échéant, en présence d'une personne de confiance désignée par ce dernier.**

**Afin d'informer le destinataire sur l'utilisation à des fins exclusivement professionnelles du système de messagerie électronique, un avertissement adéquat devrait figurer dans les messages envoyés par l'employé.**

6. *Enregistrement des données*

6.1. L'enregistrement de données à caractère personnel n'est possible que si les données ont été collectées conformément aux règles définies au paragraphe **5** et si l'enregistrement est réalisé à des fins d'emploi. **En cas de manquement à ces règles, l'employeur doit s'abstenir d'utiliser les données en question.**

6.2. Les données enregistrées devraient être exactes, mises à jour si nécessaire, et reproduire fidèlement la situation de l'employé. Elles ne devraient pas être enregistrées ou codées d'une manière qui puisse porter atteinte aux droits de l'employé en permettant de le caractériser ou d'établir son profil sans qu'il en ait connaissance.

**Si l'utilisation des données biométriques est permise aux termes du paragraphe 5.5., elles ne devraient pas, en principe, être enregistrées dans une base de données, la préférence devant être accordée, selon les cas, à des systèmes d'identification ou d'authentification biométrique basés sur des supports mis à la disposition exclusive de l'intéressé.**

6.3. Lorsque des données appréciatives relatives à la productivité ou à la potentialité des employés sont enregistrées, elles devraient être fondées sur des évaluations équitables et loyales ; elles ne doivent pas être insultantes dans la manière dont elles sont formulées.

7. *Utilisation interne des données*

7.1. Les données à caractère personnel collectées à des fins d'emploi ne devraient être utilisées par l'employeur qu'à de telles fins.

**Dans le respect des principes de pertinence et d'exactitude, notamment eu égard à des entreprises de grande dimension ou dispersées sur le territoire, l'accès à certaines données à caractère personnel pourrait être facilité sur les réseaux de communication interne afin que la prestation de travail soit exécutée avec davantage de célérité et pour faciliter l'interaction avec les autres employés.**

7.2. Lorsque des données doivent être utilisées à des fins d'emploi autres que celles pour lesquelles elles ont été initialement collectées, des mesures appropriées devraient être prises pour éviter que ces données ne soient mal interprétées dans un contexte différent et pour assurer qu'elles ne soient pas utilisées de manière incompatible avec le but initial. En cas de décision importante concernant l'employé, fondée sur des données ainsi utilisées, celui-ci devrait en être avisé.

7.3. Les dispositions du paragraphe 7.2 s'appliquent à la mise en relation de fichiers contenant des données à caractère personnel collectées et enregistrées à des fins d'emploi.

**7.4. Sans préjudice des dispositions de l'article 9, en cas de changements au sein de la société, de fusions et d'acquisitions, il convient de veiller au respect du principe de finalité dans l'utilisation des données, notamment eu égard à d'éventuelles modifications des modalités de traitement des données dont les intéressés doivent être informés.**

8. *Communication de données et utilisation de systèmes d'information aux fins de représentation des employés*

8.1. Conformément aux législations et pratiques nationales et aux conventions collectives, des données à caractère personnel peuvent être communiquées aux représentants des employés, dans la mesure où de telles données sont nécessaires pour permettre à ces derniers de représenter les intérêts des employés.

**8.2. L'utilisation de systèmes d'information pour des communications à caractère syndical devrait faire l'objet d'accords spécifiques avec l'employeur, visant à définir au préalable des règles transparentes permettant une utilisation appropriée, ainsi qu'à identifier des garanties à titre de protection d'éventuelles communications confidentielles.**

9. *Communication externe **et diffusion** des données*

9.1. Les données à caractère personnel collectées à des fins d'emploi ne devraient être communiquées à des organismes publics pour les besoins de leurs fonctions officielles que dans les limites des obligations légales de l'employeur ou conformément à d'autres dispositions du droit interne.

9.2. La communication de données personnelles à des organismes publics à des fins autres que l'exercice de leurs fonctions officielles ou à des parties autres que des organismes publics, y compris les entreprises du même groupe, ne devrait s'effectuer que :

a. lorsque la communication est nécessaire à des fins d'emploi qui ne seraient pas incompatibles avec les finalités pour lesquelles les données ont été collectées à l'origine et si les employés ou leurs représentants en sont informés ; ou

b. avec le consentement exprès et éclairé de l'employé ; ou

c. si la communication est autorisée par le droit interne, **notamment si cela s'avère nécessaire en cas d'action en justice ou en vue de l'exercice d'un droit devant une instance judiciaire.**

**9.3. En cas de consentement de l'employé ou en fonction de garanties appropriées prévues par la législation nationale, des données à caractère personnel peuvent faire l'objet d'une communication dans le cadre de groupes de sociétés afin d'exécuter les obligations prévues par la loi ou par la convention collective en matière de travail, de prévoyance et de sécurité sociale pour les employés, c'est-à-dire pour permettre la meilleure affectation de ressources humaines.**

**9.4. Concernant le secteur public, la loi devrait concilier le droit au respect de la vie privée et à la protection des données avec les exigences de transparence ou de contrôle en cas d'utilisation de ressources et de fonds publics, en distinguant des catégories ou des profils professionnels pour lesquels il est nécessaire de publier certaines informations, ainsi que la typologie des informations pertinentes qui peuvent être rendues publiques, en fonction de classes homogènes et ce, en tenant compte de la possibilité d'en prendre connaissance plus facilement s'il est possible de les retrouver à l'aide de moteurs de recherche externes.**

**9.5. Dans le cas de fonctions professionnelles impliquant des relations constantes avec le public ou lorsque des exigences de transparence à l'égard des usagers, des consommateurs et des citoyens le rendent nécessaire, il est possible d'adopter des mesures et des garanties appropriées pour rendre directement ou indirectement identifiable l'employé concerné, dès lors qu'il suffit de connaître directement un code d'identification attribué à l'employé ou une autre référence personnelle.**

*10. Flux transfrontières de données*

10.1. La communication transfrontière de données à caractère personnel collectées et enregistrées à des fins d'emploi devrait être régie par les principes énoncés aux paragraphes **7 et 9**.

*11. Catégories particulières de données*

11.1. Les données à caractère personnel révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, les données relatives à la vie sexuelle ou à des

condamnations pénales, visées à l'article 6 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, ne devraient être collectées et enregistrées que dans des cas particuliers, **lorsque cela est indispensable à l'exécution des prestations dérivant du contrat de travail**, dans les limites prévues par le droit interne et conformément aux garanties appropriées y figurant. En l'absence de telles garanties, ces données ne devraient être collectées et enregistrées qu'avec le consentement exprès et éclairé des employés.

11.2. Un employé ou un candidat à un emploi ne peut être interrogé sur son état de santé et faire l'objet d'un examen médical qu'aux fins suivantes :

a. déterminer son aptitude à un emploi actuel ou futur ;

b. couvrir les besoins de la médecine préventive ; ou

c. octroyer des prestations sociales.

**En principe, il devrait être interdit de collecter et d'utiliser des données génétiques pour déterminer le comportement professionnel des employés ou des candidats lors de l'instauration d'un contrat de travail, même avec le consentement de l'intéressé. Des dérogations exceptionnelles pourraient être prévues dans les seules limites prévues par le droit national et en présence de garanties appropriées et documentées qui devraient également prévoir une participation préventive des autorités de contrôle, uniquement afin d'adopter, à la demande l'employé, les mesures nécessaires à l'amélioration de son état de santé, de ses conditions de sécurité ou de ses fonctions.**

11.3. Les données de santé **et, en tout état de cause, les données génétiques** ne peuvent être collectées auprès d'autres sources que l'employé lui-même sans le consentement exprès et éclairé de ce dernier ou conformément aux dispositions du droit interne.

11.4. Les données de santé couvertes par le secret **médical et, en tout état de cause, les données génétiques**, devraient **être traitées exclusivement** par le personnel soumis aux règles sur le secret médical. Ces informations ne devraient être communiquées à des membres du service du personnel que si cela est indispensable à la prise de décisions par ce service et conformément au droit interne.

11.5. Les données de santé couvertes par le secret médical **et, si nécessaire, les données génétiques dont le traitement est autorisé**, devraient être enregistrées séparément des autres catégories de données détenues par l'employeur. Des mesures de sécurité devraient être prises pour éviter que des personnes étrangères au service médical n'aient accès à ces données.

11.6. Le droit d'accès de la personne concernée à ses données médicales ne devrait pas faire l'objet de restrictions, à moins que l'accès à de telles données ne puisse porter une grave atteinte à la personne concernée; dans ce cas, ces données pourraient lui être communiquées par l'intermédiaire du médecin de son choix.

**11.7. L'employeur devrait traiter les éventuelles données sur la santé relatives à des tiers si cela est indispensable à l'exécution des obligations prévues par la loi ou par la convention collective, dans le respect des garanties prévues pour les données sur la santé des employés.**

## 12. *Transparence du traitement*

12.1. Des informations sur les données à caractère personnel détenues par l'employeur devraient être mises à la disposition du travailleur concerné, soit directement, soit par l'intermédiaire de ses

représentants, ou être portées à sa connaissance par d'autres moyens appropriés. Ces informations devraient spécifier les principales finalités de ces données, le type de données enregistrées, les catégories de personnes ou d'organes auxquels les données sont régulièrement communiquées, les finalités et la base juridique de cette communication.

**Dans ce contexte, une description particulièrement claire et complète devrait être fournie relativement à la typologie des données à caractère personnel qui peuvent être collectées au moyen de systèmes d'information, de programmes ou de dispositifs électroniques permettant à l'employeur de les contrôler indirectement, ainsi que sur leur utilisation potentielle. Une description semblable devrait être fournie concernant l'emploi de technologies de Radio Frequency Identification (RFID), l'éventuelle utilisation de codes d'identification personnels, ainsi que concernant le rôle des éventuels administrateurs de système par rapport au traitement des données.**

12.2. Ces informations devraient également faire mention des droits de l'employé au regard de ses données, tels qu'ils sont prévus au paragraphe 13 de la présente recommandation, ainsi que des modalités d'exercice du droit d'accès.

**12.3. Les informations indiquées aux termes des paragraphes précédents devraient être fournies et mises à jour en temps utile et, en tout état de cause, avant que l'employé ne réalise l'activité ou le comportement qui est visé, puis mises à disposition au moyen de systèmes d'information habituellement utilisés par l'employé.**

13. *Droit d'accès et de rectification*

13.1. Tout employé devrait pouvoir avoir accès, sur demande, à toutes les données à caractère personnel le concernant détenues par son employeur, et obtenir, le cas échéant, la rectification ou l'effacement de telles données lorsque ces dernières sont détenues en contravention des principes posés dans la présente recommandation. **Il devrait également se voir reconnaître le droit de connaître leur origine et l'identité des personnes auxquelles les données ont été ou sont susceptibles d'être communiquées.**

**Á cette fin, particulièrement dans les lieux de travail de grande dimension ou dispersés sur le territoire, l'employeur devrait prévoir des procédures préventives d'ordre général afin de garantir que le contrôle soit adéquat et rapide en cas d'exercice de ces droits.**

**13.2. L'employé devrait également avoir accès aux données à caractère personnel d'ordre appréciatif, y compris celles relatives aux appréciations de la productivité ou du potentiel de l'employé, prévues au paragraphe 5.3., au moins lorsque le processus d'appréciation est terminé, le besoin de l'employeur ou de tiers de se défendre étant temporairement écarté ; même si l'employeur ne les rectifie pas directement, les appréciations purement subjectives devraient pouvoir être contestées selon les modalités prévues par le droit national.**

13.3. Dans le cas d'une enquête interne effectuée par l'employeur, l'exercice des droits mentionnés au paragraphe 13.1 peut être différé jusqu'à la conclusion de cette enquête, si cet exercice risque de nuire au résultat de l'enquête. **Cependant, un signalement anonyme ne saurait être à l'origine d'enquêtes internes, sauf si ce signalement est circonstancié et concerne de graves violations identifiées par le droit national ou par une décision de l'autorité de contrôle.**

13.4. Lorsqu'une décision découlant d'un traitement automatisé des données détenues par l'employeur est opposée à l'employé, ce dernier devrait avoir le droit de s'assurer que ces données ont été licitement traitées.

13.5. Sauf dispositions nationales contraires, l'employé devrait pouvoir désigner une personne de son choix pour l'assister lors de l'exercice de son droit d'accès ou pour exercer ce droit en son nom.

13.6. Si un employé se voit refuser l'accès aux données le concernant ou la possibilité de rectifier ou d'effacer certaines de ces données, une voie de recours devrait être prévue par le droit interne.

*14. Sécurité des données*

14.1. Les employeurs ou les entreprises auprès desquelles les données peuvent être sous-traitées devraient mettre en œuvre des mesures techniques et organisationnelles appropriées **et constamment mises à jour par rapport au développement des nouvelles technologies** pour garantir la sécurité et la confidentialité des données à caractère personnel enregistrées à des fins d'emploi, contre tout accès, utilisation, communication ou modification non autorisés.

14.2. Le service du personnel ainsi que toute autre personne intervenant dans le traitement des données devraient être tenus informés de ces mesures et de la nécessité de les respecter.

*15. Conservation des données*

15.1. Un employeur ne devrait pas conserver des données à caractère personnel pendant une période plus longue que ne le justifient les finalités définies au paragraphe 1.3 ou que ne le nécessite l'intérêt d'un employé actuel ou d'un ancien employé.

15.2. Les données à caractère personnel fournies à la suite d'un acte de candidature devraient en principe être effacées dès qu'il devient clair qu'une offre d'emploi n'interviendra pas.

15.3. Lorsque de telles données sont conservées en vue d'une demande d'emploi ultérieure, **l'intéressé devrait en être informé en temps utile et** les données devraient être effacées à sa demande.

Lorsque, pour soutenir d'éventuelles actions en justice, il est nécessaire de conserver les données fournies à l'occasion d'une candidature, ces données ne devraient être conservées que pendant une période raisonnable.

**15.4. Les données à caractère personnel enregistrées du fait d'une enquête interne réalisée par l'employeur et qui n'a entraîné l'adoption d'aucune mesure négative à l'égard des employés devraient, en principe, être effacées en temps utile, sous réserve du droit d'accès jusqu'au moment où elles seront effacées.**