COMMITTEE OF MINISTERS
COMITÉ DES MINISTRES
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Délégués des Ministres
Documents CM

CM(2015)32 addfinal 1 avril 2015[1]

1224 Réunion, 1er avril 2015

5 Media

5.1 Comité directeur sur les médias et la société de l'information (CDMSI)

a. Recommandation CM/Rec(2015)5 du Comité des Ministres aux Etats membres sur le traitement des données à caractère personnel dans le cadre de l'emploi – Exposé des motifs

EXPOSÉ DES MOTIFS

de la Recommandation CM/Rec(2015)5
du Comité des Ministres aux Etats membres
sur le traitement des données à caractère personnel dans le cadre de l'emploi

(adoptée par le Comité des Ministres le 1er avril 2015
lors de la 1224e réunion des Délégués des Ministres)

Introduction

1. La Recommandation n° R (89) 2 du Comité des Ministres aux Etats membres sur la protection des données à caractère personnel utilisées à des fins d'emploi était le sixième instrument de la sorte adopté par le Comité des Ministres dans le cadre d'une approche sectorielle des questions relatives à la protection des données.

2. Vingt-cinq ans ont passé depuis l'adoption de cette recommandation. Le travail en soi s'est profondément transformé (tant son objet que sa forme, sa durée et ses intermédiaires), tout comme ont évolué son cadre physique et son organisation. Les employeurs, les employés et leurs besoins ont changé et, du fait de l'utilisation accrue des nouvelles technologies, l'éventail des données à caractère personnel traitées s'est élargi (adresse IP, fichier journal, géolocalisation, par exemple). Il était donc nécessaire de réviser la recommandation.

3. En 2011, le Comité consultatif de la Convention n° 108 a confié à un expert le soin de réaliser une étude sur la recommandation n° R (89) 2 et de soumettre des propositions de révision en la matière (document T-PD-BUR(2010)1FIN – « Etude sur la Recommandation n° R (89) 2 sur la protection des données à caractère personnel utilisées à des fins d'emploi – propositions de révision de la recommandation ci-mentionnée », par Giovanni Buttarelli).

4. Sur la base de cette étude, le comité consultatif s'est employé à réviser la recommandation. Il a approuvé le projet de texte à sa 31e réunion plénière (2-4 juin 2014). Il a ensuite transmis le projet de recommandation révisée au Comité directeur sur les médias et la société de l'information (CDMSI) en vue de son examen et de son approbation, ce qui a permis une consultation parallèle du Comité européen de coopération juridique (CDCJ).

[1] Ce document a été classé en diffusion restreinte jusqu'à la date de son examen par le Comité des Ministres.
Internet : http://www.coe.int/cm

5. En ce qui concerne l'évolution du contexte par rapport à 1989, les éléments suivants ont été pris en compte :

- l'utilisation croissante des technologies de l'information dans le cadre de l'emploi et la nécessité de protéger la dignité et les droits fondamentaux de l'employé face au contrôle de ses activités ;
- la tendance des employeurs à recueillir des données sur les employés en dehors du strict périmètre du travail, par exemple dans les moteurs de recherche et sur les réseaux sociaux ;
- l'introduction de formes particulières de traitement comportant des risques particuliers pour les individus et utilisant par exemple les données biométriques ou de géolocalisation.

6. Le projet de recommandation a été approuvé par le CDMSI lors de sa 7e réunion (18-21 novembre 2014).

7. La Recommandation CM/Rec(2015)5 du Comité des Ministres aux Etats membres sur le traitement des données à caractère personnel dans le cadre de l'emploi a été adoptée par le Comité des Ministres du Conseil de l'Europe le 1er avril 2015.

Préambule

8. Le préambule énonce les raisons qui ont conduit le Comité des Ministres à présenter la recommandation aux gouvernements des Etats membres.

9. L'action du Conseil de l'Europe dans le domaine de la protection des données est toujours partie du principe que les technologies de l'information et de la communication (TIC) apportent des avantages incontestables à la société. Le principal souci de l'Organisation dans ce contexte a été de définir des normes qui prennent en compte les progrès technologiques, tout en reconnaissant clairement la nécessité de protéger les intérêts des personnes, s'agissant notamment du traitement des données.

10. Le secteur de l'emploi, privé et public – auquel les principes de la présente recommandation s'adressent – reflète cette préoccupation : comment concilier les avantages indéniables que la technologie apporte aux entreprises et les droits et les libertés des employés dans un environnement de travail où les TIC font partie intégrante des activités quotidiennes des employés ? Les avantages que ces technologies leur apportent en termes d'amélioration de l'organisation du travail, de réduction des opérations courantes, etc., doivent être évalués à la lumière de l'impact éventuel sur la vie privée qui peut en découler pour l'employé et pour tous les effectifs d'une entité dans son entier. Le préambule reconnaît également que l'introduction des TIC sur le lieu de travail peut représenter un risque pour d'autres droits et libertés – la liberté d'association ou la liberté d'expression, par exemple, telles que garanties par la Convention de sauvegarde des droits de l'homme et des libertés fondamentales [plus connue sous le nom de Convention européenne des droits de l'homme] (STE n° 5, ci-après «la CEDH »), ainsi que les droits garantis par la Charte sociale européenne, qui concernent directement la relation entre employeurs et employés.

11. Le premier paragraphe de l'article 8 de la CEDH dispose que « toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance ». La Cour européenne des droits de l'homme (ci-après « la Cour ») a également développé une jurisprudence selon laquelle l'article 8 peut également créer des obligations positives inhérentes au « respect » effectif de la vie privée. Compte tenu de ces obligations positives, l'Etat doit prendre les mesures nécessaires, y compris législatives, pour garantir dans la pratique le respect effectif des droits découlant de l'article 8 de la CEDH.

12. Il est d'emblée précisé que le droit au respect de la vie privée d'un employé ne saurait s'interpréter uniquement comme le droit d'être protégé de toute intrusion injustifiée dans sa vie professionnelle quotidienne, même si les principes de la recommandation relatifs au contrôle et à la surveillance des employés sont étroitement liés à cette acception traditionnelle de la notion de vie privée. Au contraire, les principes énoncés reflètent les préoccupations exprimées dans les dispositions de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108, ci-après la « Convention n° 108 »), datée du 28 janvier 1981, visant à protéger les personnes concernées en réglementant le traitement (collecte, utilisation, conservation, etc.) des informations personnelles.

13. La recommandation est donc structurée de sorte à appliquer les principes généraux de la Convention n° 108 au contexte de l'emploi en énonçant des principes qui visent à réglementer les activités pertinentes de l'employeur. En d'autres termes, en adaptant les principes fondamentaux de la Convention n° 108 relatifs à la loyauté et la licéité du traitement des données, à la détermination des finalités, à la proportionnalité et à la minimisation des données, et à l'accès aux données, les lignes directrices contenues dans la recommandation permettent de répondre à des questions telles que celles-ci : comment les employeurs devraient-ils recueillir les données ? Pour quelles finalités ? Comment les données conservées peuvent-elles être utilisées ? Quels droits les employés ont-ils sur les données traitées par l'employeur ?

14. Etant donné que la recommandation incarne une approche sectorielle de la protection des données, il convient de prendre en compte l'ensemble des éléments qui distinguent le secteur en question et influencent la

manière dont les principes fondamentaux de la Convention n° 108 seront adaptés. En conséquence, le texte s'efforce de prendre en considération les besoins légitimes types de l'employeur en matière d'information, ainsi que les besoins légitimes de l'employé en matière de vie privée/protection des données. Toutefois, comme l'indique le préambule, le secteur de l'emploi a également pour caractéristique de mettre en jeu à la fois des intérêts collectifs et des intérêts individuels. Pour être valable, l'approche sectorielle doit également avoir pour objectif d'adapter les principes généraux de la Convention n° 108 à la réalité de l'intérêt collectif. C'est pourquoi est acquise la possibilité, à différents stades de la recommandation, d'avoir des représentants qui défendent les intérêts des employés en matière de protection des données, au niveau individuel ou au nom de tous les employés d'une entité.

15. En ce qui concerne la mise en œuvre des principes de la recommandation, les gouvernements des Etats membres devraient s'assurer de la prise en compte des principes énoncés à l'annexe de la recommandation dans l'application de la législation nationale sur la protection des données dans le secteur de l'emploi, ainsi que dans d'autres branches du droit qui ont une incidence sur l'utilisation des données à caractère personnel à des fins d'emploi.

16. Le dispositif de la recommandation prévoit plusieurs façons de mettre en œuvre ces principes. En premier lieu, les autorités établies conformément à la législation nationale en matière de protection de données peuvent se prévaloir de ces principes lorsqu'il existe des problèmes de protection des données dans le cadre de relations entre employeurs et employés. Les gouvernements des Etats membres devraient, par conséquent, s'assurer que ces autorités ont conscience de l'existence de la recommandation et de son intérêt pour régler les conflits dans ce secteur. La Convention n° 108, à laquelle les normes nationales se conforment, ne prévoit aucune exception pour le secteur de l'emploi. Ainsi, les autorités chargées de l'application des normes nationales en matière de protection des données peuvent-elles invoquer les dispositions de la recommandation pour appliquer les normes relatives à la protection des données dans le secteur de l'emploi. A titre d'exemple, elles peuvent appliquer les principes énoncés dans la recommandation dans des cas concrets ou les utiliser comme point de départ pour élaborer les codes de conduite proposés dans le domaine de l'emploi. La Recommandation CM/Rec(2010)13 du Comité des Ministres aux Etats membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, qui énonce les règles régissant le traitement des données à caractère personnel dans ce cadre, peut se révéler particulièrement pertinente dans le contexte de l'emploi.

17. Outre ces considérations, la recommandation estime que les partenaires sociaux eux-mêmes peuvent négocier l'acceptation et le respect de ces principes, soit pour compléter la réglementation juridique en place, soit pour s'y substituer. Le préambule prend en compte la diversité des approches nationales en matière d'intervention de l'Etat dans les relations de travail qui peut varier d'une réglementation plus ou moins forte à la libre négociation collective – c'est-à-dire en dehors de toute intervention de l'Etat – entre les partenaires sociaux pour les questions relatives aux rapports employeurs-employés. En conséquence, en l'absence d'initiatives législatives visant à mettre en œuvre les principes de la recommandation, les gouvernements devraient s'assurer que les organes représentatifs des employeurs et des employés sont dûment informés de l'intérêt de l'approche adoptée par la recommandation en matière de protection des données.

Annexe à la Recommandation CM/Rec(2015)5

Partie I – Principes généraux

1. Champ d'application

18. Conformément au champ d'application de la Convention n° 108, les principes de la recommandation s'appliquent au traitement des données à caractère personnel à des fins d'emploi dans les secteurs public et privé. Par « à des fins d'emploi » est entendu tout un éventail d'activités de traitement (voir ci-après) liées au recrutement, à l'exécution du contrat de travail, à l'exécution des obligations découlant de la loi ou de conventions collectives, à la planification de la gestion et à l'organisation du travail, à l'égalité et à la diversité sur le lieu de travail, à la santé et la sécurité au travail, à la protection des biens des employeurs et des clients, à l'exercice et à la jouissance, à titre individuel ou collectif, des droits et avantages liés à l'emploi et à la cessation de la relation de travail.

19. Certaines dispositions (« sauf législations nationales contraires ») du principe 1.2 de la recommandation s'appliquent aux activités des agences pour l'emploi ou des cabinets de recrutement dans les secteurs public et privé. Il peut arriver que certains pays membres considèrent les agences publiques pour l'emploi dans un contexte autre que celui de l'emploi et les réglementent en dehors du champ d'application du droit du travail – par exemple par la législation sur la sécurité sociale. Néanmoins, même si ces pays choisissent de ne pas appliquer les principes de la recommandation à leurs activités, leur législation générale en matière de protection des données ne manquera pas de s'appliquer à leurs activités de traitement des données.

20. En vertu du principe 1.2, les agences pour l'emploi exploitent les données en leur qualité de responsables du traitement ou de sous-traitants, conformément aux principes de la présente recommandation et uniquement aux fins initialement prévues. Dans certains cas, les agences pour l'emploi utilisent les données des candidats pour faciliter les démarches des employeurs liées à l'établissement des contrats de travail.

2. Définitions

21. La définition de l'expression « données à caractère personnel » concorde avec celle de la Convention n° 108. Il s'agit d'une définition établie de longue date qui a été réaffirmée au fil du temps dans divers instruments juridiques du Conseil de l'Europe. L'expression « données à caractère personnel » est définie de manière large et devrait être interprétée de sorte à prendre également en compte l'utilisation croissante des nouvelles technologies et des moyens de communication électronique dans le cadre des relations entre employeurs et employés. Les données à caractère personnel peuvent englober le nom d'un employé, son âge, son adresse, son statut marital, sa formation, des « fichiers journaux », etc. Elles peuvent aussi inclure des évaluations de l'employeur ou son avis sur l'employé, voire une image numérisée de ce dernier.

22. La définition de l'expression « données à caractère personnel » renvoie à toute information sur une personne physique identifiée ou identifiable. Une personne dite « identifiable » est une personne susceptible d'être identifiée directement ou indirectement. Une personne n'est pas considérée comme « identifiable » si son identification nécessite un délai, des activités ou des moyens déraisonnables. La détermination de ce que constitue « un délai, des activités ou des moyens déraisonnables » devrait se faire au cas par cas, au regard de la finalité du traitement des données et en tenant compte de critères objectifs tels que le rapport coût-avantages du processus d'identification, la technologie utilisée et disponible au moment du traitement, ainsi que les développements technologiques, etc.

23. Les données qui semblent anonymes car non assorties d'identificateurs flagrants peuvent néanmoins, dans des cas particuliers, permettre d'identifier la personne concernée. Tel est par exemple le cas lorsque, de façon séparée ou en regroupant des données physiques, physiologiques, génétiques, psychologiques, économiques, culturelles ou sociales (âge, sexe, profession, géolocalisation, statut familial, etc.), le responsable du traitement ou tout autre acteur légitime ou illégitime (en particulier lorsque les données ont été rendues publiques) peuvent identifier la personne concernée. Dans ce cas, les données ne sont plus considérées comme anonymes et doivent donc être traitées comme des données à caractère personnel.

24. L'expression « traitement des données » recouvre une notion générale ouverte qui peut être interprétée de manière souple et commence par la collecte ou la création de données à caractère personnel, et englobe l'ensemble des opérations automatisées, que ce soit partiellement ou en totalité. On parle également de traitement de données lorsqu'aucun procédé automatisé n'est utilisé mais que les données sont structurées de manière à permettre la recherche, la combinaison ou la corrélation de données sur tel ou tel employé ou candidat à l'emploi.

25. L'expression « systèmes d'information » renvoie à tout type de dispositif tel que les ordinateurs, les caméras, le matériel vidéo, les dispositifs sonores, les téléphones et autres équipements de communication, ainsi que diverses méthodes d'établissement de l'identité et de la localisation, ou toute méthode de surveillance. Les termes « outils » et « dispositifs » entrent dans la notion de « systèmes d'information » et de technologies de l'information, dont la définition est donnée dans la recommandation.

26. En ce qui concerne la notion « à des fins d'emploi », il convient de souligner que le principe de finalité ou de détermination de la finalité est ici essentiel puisqu'il sert à définir et à restreindre les activités de l'employeur visant à recueillir des informations à caractère personnel. Comme le prévoit la Convention n° 108, les données à caractère personnel traitées doivent être recueillies pour des finalités explicites, déterminées et légitimes, et ne doivent pas être utilisées de manière incompatible avec ces finalités. La finalité déterminée pour ce secteur – « à des fins d'emploi » – vise à concilier les intérêts de l'employeur avec ceux des employés, tout en acceptant que l'employeur puisse servir d'intermédiaire entre l'Etat et l'employé aux fins de la collecte et de la conservation de données à caractère personnel, pour transmission ultérieure à l'Etat – par exemple conformément au droit fiscal ou à la législation sur la sécurité sociale ou la sécurité industrielle (« l'exécution des obligations découlant de la loi »).

27. L'expression « à des fins d'emploi » couvre également le cadre disciplinaire (enquêtes et sanctions internes, par exemple) ainsi que les données traitées après la résiliation du contrat de travail. Il convient d'établir

clairement que, en cas de conservation des données après la fin du contrat, le traitement devra être conforme au principe 13 et au principe de finalité. L'expression « contrat de travail » s'entend de tout accord, oral ou écrit, exprimé ou supposé, qui précise les conditions et modalités dans lesquelles une personne consent à exécuter certaines tâches sous la direction et le contrôle d'un employeur, habituellement, mais pas toujours, en contrepartie d'une rémunération ou d'un salaire convenu(e) au préalable. Il est entendu que, pour les rédacteurs de la recommandation, ce terme de « contrat de travail » renvoie également aux emplois non rémunérés, par exemple au titre du bénévolat, d'un stage ou de la formation. Les principes de la recommandation s'appliquent donc également aux personnes engagées dans une relation de travail au titre de ces statuts. En outre, la relation de travail dans le secteur public doit être garantie, sans toutefois reposer nécessairement sur un contrat de travail. Les modalités, conditions et devoirs découlant de l'emploi sont généralement précisés conformément aux réglementations pertinentes du droit administratif.

28. L'« employeur » est une entité légale qui contrôle et dirige un employé dans le cadre d'une relation de travail, généralement quand une personne exécute une tâche ou fournit des services dans certaines conditions et en contrepartie d'une rémunération. La relation de travail crée des droits et obligations réciproques entre l'employé et l'employeur. Elle a toujours été, et continue d'être, le principal moyen par lequel les travailleurs ont accès aux droits et avantages associés à l'emploi dans le droit du travail et dans le domaine de la sécurité sociale[2].

29. L'« employé » est une personne recrutée pour s'acquitter d'une tâche en faveur de l'employeur dans le cadre d'une relation de travail. Les termes « travailleur » ou « agent » renvoient également à la définition d'« employé ». Une attention particulière doit être accordée à la notion d'employé. A cet égard, il convient de se référer à l'arrêt de la Cour de justice de l'Union européenne (CJUE) dans l'affaire C-94/07 - *Andrea Raccanelli c. Max-Planck-Gesellschaft zur Förderung der Wissenschaften eV*. La CJUE a en effet statué que « la notion de "travailleur", au sens de l'article 35 du Traité sur le fonctionnement de l'Union européenne, revêt une portée spécifique et ne doit pas être interprétée de manière restrictive. Doit être considérée comme « travailleur » toute personne qui exerce des activités réelles et effectives, à l'exclusion d'activités tellement réduites qu'elles se présentent comme purement marginales et accessoires. La caractéristique de la relation de travail est, selon cette jurisprudence, le fait qu'une personne accomplit pendant un certain temps, en faveur d'une autre personne et sous la direction de celle-ci, des prestations en contrepartie desquelles elle touche une rémunération.

30. Les candidats à l'emploi doivent bénéficier de la même protection et des mêmes droits que les employés, même si leur candidature ne débouche pas sur un contrat de travail. De même, il convient de souligner que les principes de la présente recommandation s'appliquent également aux anciens employés.

3. Respect des droits de l'homme, de la dignité humaine et des libertés fondamentales

31. Le principe 3 constitue une affirmation générale sur laquelle se fonde le reste de la recommandation pour aborder la question du traitement des données à caractère personnel dans le domaine de l'emploi. La vie privée doit être considérée sous l'angle de la protection des données et comme imposant des restrictions au traitement des informations à caractère personnel par les employeurs. Dans ce sens, elle doit également être considérée comme conférant des droits positifs aux employés, leur permettant ainsi de contrôler, en vertu des droits prévus au principe 11, que les employeurs ont bien respecté leurs obligations en matière de protection des données.

32. La référence à la « dignité humaine » dans le texte tient compte du fait que la technologie ne devrait pas être utilisée de sorte à empêcher l'interaction sociale des employés. Ces préoccupations sont prises en compte ultérieurement dans le texte.

33. L'approche adoptée est cohérente avec la position de la Cour européenne des droits de l'homme, qui n'a cessé de répéter qu'il est difficile de séparer complètement la vie privée de la vie professionnelle. Dans l'affaire *Niemietz c. Allemagne*[3], relative à la perquisition du bureau du requérant par une autorité publique, la Cour a estimé qu'une telle opération était contraire à l'article 8, affirmant que « [l]e respect de la vie privée doit aussi englober, dans une certaine mesure, le droit pour l'individu de nouer et développer des relations avec ses semblables. Il paraît, en outre, n'y avoir aucune raison de principe de considérer cette manière de comprendre la notion de "vie privée" comme excluant les activités professionnelles ou commerciales : après tout, c'est dans leur travail que la majorité des gens ont beaucoup, voire le maximum d'occasions de resserrer leurs liens avec le monde extérieur. Un fait, souligné par la Commission, le confirme : dans les occupations de quelqu'un, on ne peut pas toujours démêler ce qui relève du domaine professionnel de ce qui en sort ».

34. Par ailleurs, dans l'affaire *Halford c. Royaume-Uni*[4], la Cour a estimé que l'interception des communications téléphoniques des employés emportait violation de l'article 8 de la Convention. Elle a en effet conclu que « les appels téléphoniques émanant de locaux professionnels, tout comme ceux provenant du

[2] Source OIT : http://www.ilo.org/ifpdial/areas-of-work/labour-law/WCMS_CON_TXT_IFPDIAL_EMPREL_EN/lang--en/index.htm
[3] *Niemietz c. Allemagne*, Requête n° 13710/88, 16 décembre 1992.
[4] *Halford c. Royaume-Uni*, Requête n° 20605/92, 25 juin 1997.

domicile, peuvent se trouver compris dans les notions de “vie privée" et de “correspondance” visées à l’article 8, paragraphe 1 (…) ».

35. Dans l’arrêt *Copland c. Royaume-Uni*[5], la Cour a réaffirmé cette position en ce qui concerne la surveillance des appels téléphoniques, des messages électroniques et des connexions à l’internet d’un employé. La Cour a estimé que la collecte et le stockage d’informations à caractère personnel relatives à M^me^ Copland, par le biais de la surveillance de ses appels téléphoniques, de son courrier électronique et de son usage de l’internet, constituaient des ingérences dans l’exercice de son droit au respect de sa vie privée et de sa correspondance, et que ces ingérences n’étaient pas « prévues par la loi », faute à l’époque de texte de droit interne réglementant les mesures de surveillance. La Cour a reconnu qu’il pouvait parfois être légitime pour un employeur de surveiller et de contrôler l’usage fait par un employé de son téléphone et d’internet, mais, dans le cas présent, elle n’était pas amenée à se prononcer sur le caractère nécessaire de l’ingérence, dans une société démocratique.

4. Application des principes de protection des données à caractère personnel

36. Les systèmes et technologies de l’information servant au traitement des données à caractère personnel dans le cadre de l’emploi devraient être utilisés de sorte à réduire au minimum le traitement des données à caractère personnel et à restreindre l’utilisation des données identifiant ou permettant d’identifier des personnes à ce qui est strictement nécessaire pour atteindre les objectifs déterminés dans les cas individuels concernés.

37. En vertu du principe 4.2, les employeurs devraient adopter des mesures appropriées pour garantir qu’ils respectent en pratique les principes et obligations en matière de traitement des données à des fins d’emploi. Les employeurs devraient en outre être en mesure de démontrer aux autorités de contrôle compétentes qu’ils se conforment à ces principes. Enfin, les employeurs devraient prendre des mesures pour garantir le respect des règles en matière de protection des données dans le cadre des opérations de traitement et conserver la trace de tous les types de traitement des données à caractère personnel relevant de leur responsabilité, afin de prouver aux employés et aux autorités de contrôle que des mesures ont été prises pour se conformer aux règles en matière de protection des données.

38. Il convient également de souligner que les principes relatifs à la protection des données devraient aussi être respectés dans le cadre du développement et de l’utilisation des technologies, et que les principes de la Convention n° 108 sont pleinement applicables à cet égard (notamment ceux qui portent sur la qualité des données, les données sensibles, la sécurité des données et les droits des personnes concernées). L’expérience a montré que, dans le contexte de l’emploi, l’employeur cherche à gérer efficacement son entreprise et à optimiser l’utilisation des nouvelles technologies, et ainsi à tirer profit de leur potentiel. Cela étant, ces nouvelles technologies, par exemple la vidéosurveillance, la biométrie ou la géolocalisation, permettent aux employeurs de contrôler toutes les activités de leurs employés, si la loi ne régit pas ou n’interdit pas ce type de surveillance. Nous aborderons plus loin comment respecter les principes de protection des données et trouver un juste équilibre entre les droits des employés et l’intérêt légitime de l’employeur.

39. Qui plus est, en vertu du principe 4.2, les mesures devraient être adaptées au volume et à la nature des données traitées, ainsi qu’à la portée, au contexte et à la finalité du traitement, et, à cet égard, des solutions simplifiées appropriées devraient être mises en œuvre dans les environnements de travail de taille réduite. En ce qui concerne la finalité de l’application des principes de la recommandation, le texte ne fait pas de distinction entre petites et moyennes entités, et grandes entités. Il ne considère pas la taille de l’environnement de travail comme un facteur décisif pour la protection des données puisque des problèmes peuvent se poser quel que soit le nombre d’employés. Les principes sont facilement applicables dans les environnements de travail réduits, notamment les petites entreprises familiales, avec des exigences minimales. Toutefois, la législation devrait tenir compte de la nécessité de ne pas imposer d’obligations juridiques inutiles aux petites entreprises qui traitent de petits volumes de données non sensibles.

5. Collecte et enregistrement des données

40. Le principe 5 vise à adapter certaines des dispositions de protection de l’article 5 de la Convention n° 108 à la collecte de données sur des personnes par leurs employeurs. Ce principe n’est pas restreint à la seule collecte de données sur des employés en poste. Il s’applique également aux besoins en matière de protection des données des candidats à l’emploi, même si aucune offre d’emploi ne leur a été faite. Il est jugé souhaitable de formuler des lignes directrices en matière de collecte de données au stade du recrutement également.

41. Le principe 5.1 souligne la nécessité de considérer l’employé comme première source d’information. En d’autres termes, si l’employeur sollicite des informations sur un employé donné, il doit le faire directement auprès de l’employé concerné. Il ne s’agit pas là d’une règle absolue. Les dispositions du principe 5.1 admettent qu’il puisse être nécessaire, à certains moments, de s’adresser à d’autres personnes pour obtenir des

[5] *Copland c. Royaume-Uni*, Requête n° 62617/00, 3 avril 2007.

informations sur l'employé, par exemple lorsqu'il s'agit de vérifier l'exactitude des informations fournies par un candidat à l'emploi dans le cadre d'une procédure de recrutement ou de promotion, à condition que l'employé ou le candidat à l'emploi en ait été dûment informé au préalable.

42. Il importe de souligner que, en vertu du principe 5, de nombreux aspects du traitement de données sur les employés ne nécessitent pas de consentement particulier puisqu'ils se fondent sur une autre base juridique légitime prescrite par la loi. La mesure dans laquelle le consentement individuel peut servir à justifier le traitement de données à caractère personnel dans le cadre de l'emploi a ses limites. En effet, pour être valable, le consentement doit notamment être informé, libre et limité aux cas où l'employé est face à un véritable choix et en mesure de refuser ou de retirer son consentement sans préjudice. D'une manière générale, toutes les opérations de traitement de données dans le cadre de l'emploi devraient être prévues par la législation nationale.

43. Il ressort du principe 5.2 que le volume d'informations à caractère personnel qui peut être légitimement collecté sur les employés dépend de l'emploi en question. Les employeurs devraient revoir leurs pratiques en matière de collecte de données – par exemple, le type de données requises sur les formulaires de candidature – de sorte à garantir qu'ils ne conservent pas plus d'informations personnelles que ne l'imposent la nature de l'emploi ou les besoins du moment. Le texte admet qu'à certains moments de la vie d'une entité il puisse être nécessaire, pour l'employeur, d'obtenir plus de données que d'habitude – ainsi, dans la perspective d'une fusion ou d'une restructuration générale, il peut être nécessaire de recueillir les points de vue personnels des employés. Il convient de noter à cet égard que, outre les exigences de pertinence et d'exactitude, la procédure de collecte doit également respecter le principe de proportionnalité et de traitement transparent et loyal.

44. L'utilisation de moteurs de recherche pour rassembler des données par exemple (notamment des sons, des photos, des vidéos) peut avoir une incidence importante sur la vie privée et sociale d'une personne, en particulier si les données à caractère personnel dérivées d'une recherche sont incomplètes, excessives, erronées ou obsolètes. En adoptant une démarche préventive fondée sur une logique de respect de la vie privée dès la conception, il est possible de réduire les problèmes de mise en œuvre en encourageant la distribution de produits respectant davantage la vie privée et axés, rien que d'un point de vue technique et organisationnel, sur les principes de nécessité, de minimisation des données et de proportionnalité.

45. Le principe 5.3 fait référence à la notion de « réseaux sociaux ». Un réseau social est une plate-forme qui permet à des personnes qui partagent des intérêts, des activités, des origines ou des relations dans la vie réelle de nouer des relations sociales. Il s'agit d'un service en ligne qui permet aux personnes de créer un profil, d'établir une liste d'utilisateurs avec qui partager des points de vue et de développer des relations croisées au sein du système. Les responsables des services de réseautage social sont eux-mêmes tenus de respecter les principes de la protection des données et les obligations correspondantes, notamment en termes d'information, de manquement et de proportionnalité. Toutefois, les employeurs devraient s'abstenir de recueillir des données sur des candidats à l'emploi ou des employés sans les en informer, en utilisant un intermédiaire, un autre nom ou un pseudonyme.

46. Lorsque l'accès au compte d'un employé ou d'un candidat à l'emploi sur un réseau social est restreint, l'employeur n'a pas le droit de demander à y avoir accès, par exemple en demandant à l'employé/candidat à l'emploi de lui communiquer ses identifiants de connexion.

47. Si la collecte et le traitement des données relatives à la santé sont visés au principe 9, les rédacteurs de la recommandation ont jugé important de rappeler cette règle au principe 5.4, car les données de santé sont des données sensibles et leur traitement dans le cadre de l'emploi n'est possible que si les garanties appropriées sont en place et les conditions nécessaires remplies.

48. L'enregistrement des données à caractère personnel visé au principe 5.5 se rapporte à la collecte de données. Les employeurs devraient se fonder sur des motifs légitimes pour enregistrer les données à caractère personnel qu'ils ont recueillies sur leurs employés à des fins d'emploi, et la durée pendant laquelle ces données sont conservées dépendra des impératifs liés à la finalité du traitement. Ainsi, les données collectées sur des candidatures à l'emploi ou les entretiens avec des candidats qui n'ont pas été retenus devraient être conservés pendant une période très brève (voir également paragraphes 107-108).

6. Utilisation interne des données

49. Le principe 6 porte uniquement sur les situations où les données à caractère personnel sont utilisées en interne par l'employeur. Le principe 6.1 souligne la nécessité de respecter la finalité prévue. Les données à caractère personnel collectées et conservées à des fins d'emploi ne devraient être utilisées qu'à de telles fins. Il importe d'identifier clairement les différents cas dans lesquels les données à caractère personnel peuvent être légitimement utilisées « à des fins d'emploi », et d'apporter les spécifications et garanties nécessaires. Toutefois, il convient de garder à l'esprit que l'expression « à des fins d'emploi » désigne tout un éventail de finalités secondaires pour le traitement de données. Par exemple, des données à caractère personnel peuvent être traitées aux fins de la gestion d'un programme de formation pour les employés, d'un prêt accordé par la

société ou d'un régime de retraite, ou les données peuvent concerner des candidats à une promotion, ou encore, elles peuvent être traitées pour des questions de salaire. Il est jugé important de considérer le contexte pour lequel les données sont collectées puisque l'utilisation aléatoire des données peut détourner la finalité pour laquelle les données ont été initialement recueillies, même si la finalité reste l'emploi.

50. Compte dûment tenu des principes de pertinence et d'exactitude, et eu égard en particulier aux environnements de travail de grande taille ou étendus au plan territorial, certaines données à caractère personnel telles que les adresses électroniques ou les photos peuvent être rendues facilement accessibles sur les réseaux de communication interne afin d'accélérer l'exécution du travail et de faciliter l'interaction avec les autres employés. Dans de tels cas, les employés concernés devraient être dûment informés de la communication interne de leurs données.

51. Le principe 6.2 encourage les employeurs à adopter des politiques/règles internes de protection de la vie privée et d'informer les employés en conséquence. Ces règles devraient tenir compte des principes énoncés dans la recommandation en matière de protection des données, plus particulièrement :

- le principe du traitement loyal : collecte de données directement auprès de l'employé concerné, informations fournies aux employés, exercice des droits des employés ;
- la finalité du traitement : les données devraient être collectées pour des finalités explicites, légitimes et déterminées, et ne devraient pas être utilisées à d'autres fins ;
- la communication des données : uniquement pour les finalités évoquées ci-dessus ;
- la sécurité des données : des mesures de sécurité appropriées devraient être mises en place pour empêcher l'accès non autorisé aux données, leur modification, leur divulgation ou leur destruction, ainsi que la perte ou la destruction accidentelles de ces données ;
- les mesures pour conserver des données exactes et à jour : pour empêcher la prise de décisions ou d'actions fondées sur des données inexactes ;
- les restrictions en matière d'enregistrement des données : cette exigence oblige l'employeur à préciser clairement la durée pendant laquelle les données seront conservées et la raison pour laquelle les informations sont conservées ;
- les droits des employés ;
- les obligations de l'employeur.

52. Les employeurs sont par ailleurs encouragés à adopter des procédures et/ou des politiques internes contraignantes définies avant la réalisation de nouvelles opérations de traitement des données, par exemple sur la manière de fournir des informations appropriées aux employés ou sur la manière de leur apporter des réponses appropriées lorsqu'ils exercent leurs droits ou déposent une réclamation.

53. Le principe 6.3 recommande de prendre des mesures appropriées pour garantir que le nouveau contexte dans lequel sont redéployées les données reflète dûment la nature contextuelle d'origine de la collecte des données et respecte la finalité déterminée à l'origine pour la collecte et l'enregistrement des données. Ainsi, si l'employeur entend s'appuyer sur les données de présence et d'absence des employés pour décider s'il doit ou non effectuer une retenue sur salaire pour présence irrégulière, il convient de veiller à montrer que l'absence répétée d'un employé est justifiée par le fait qu'il ou elle a été autorisé(e) à suivre une formation. A l'inverse, le fait que le dossier d'un employé révèle des arriérés dans ses remboursements d'un prêt accordé par la société ne devrait pas être pris en compte dans le cadre d'une procédure disciplinaire.

54. Par ailleurs, indépendamment des différentes conceptions de la notion d'« incompatibilité » selon les pays, il peut arriver que l'engagement pris par un employeur de ne pas utiliser à d'autres fins des données collectées pour une finalité précise dans le cadre de la relation de travail puisse effectivement restreindre l'utilisation ultérieure de ces données. Parfois, la nature même de la finalité pour laquelle les données à caractère personnel ont été collectées à l'origine (à des fins de statistiques ou de recherche sur les maladies professionnelles, par exemple) empêche l'utilisation ultérieure de ces données pour une autre finalité dans le domaine de l'emploi sans lien avec la finalité d'origine. Pour déterminer si l'utilisation ultérieure des données à caractère personnel est « incompatible » ou non avec la finalité pour laquelle les données ont été collectées à l'origine, une évaluation au cas par cas est nécessaire.

55. Le fait d'informer l'employé de toute proposition d'utilisation de données issues de différents contextes pour prendre des décisions susceptibles d'influer sur ses intérêts est considéré comme une garantie qui protège l'employé du type de préjudice illustré ci-dessus. Il s'agit d'une exigence fondamentale du principe de traitement loyal et de transparence qui régit les relations d'emploi.

56. En cas de transfert d'activités ou d'entreprises, il peut être acceptable de communiquer certaines catégories de données à caractère personnel sur les employés à des tiers (autres sociétés du même groupe, nouvel employeur en cas d'acquisition ou de fusion, transfert de contrats, par exemple). Le volume d'informations personnelles sur les employés qui peut être légitimement communiqué à des tiers dépendra bien évidemment de l'emploi en question et, outre les exigences de pertinence et de proportionnalité, la communication de ces données devra également tenir compte de la nécessité de respecter la finalité

déterminée (« à des fins d'emploi »). Lorsque le traitement est modifié de manière substantielle, les personnes concernées devraient également en être informées, conformément au droit applicable et aux règles jugées appropriées par les autorités responsables de la protection des données. Lorsque des transmissions d'entreprises ou de sociétés donnent lieu à des transferts de données relatives aux employés vers des pays tiers, ces transferts ne peuvent intervenir que si ces pays tiers assurent un niveau adéquat de protection des données ou si des garanties adéquates sont en place.

57. Le principe 6 ne dit rien sur la question du traitement des données à caractère personnel par les employeurs à des fins de recherche ou de statistiques, alors que cela peut parfois être nécessaire pour des besoins de planification et d'organisation du travail. Dans ce cas, il convient de respecter les principes énoncés dans la Recommandation n° R (83) 10 relative à la protection des données à caractère personnel utilisées à des fins de recherche scientifique et de statistiques.

7. Communication des données et utilisation des TIC pour la représentation des employés

58. La signification à attribuer à l'expression « représentants des employés » est à déterminer par la législation et la pratique nationales dans le domaine des relations du travail. Ces représentants peuvent être des comités d'entreprise, des représentants syndicaux ou d'autres associations auxquelles l'employé est affilié. Il peut parfois être nécessaire de communiquer les noms et adresses des employés à l'organe représentatif pour permettre la diffusion des documents relatifs aux élections syndicales à venir. La communication des données à caractère personnel relatives aux employés non affiliés à l'organe représentatif devrait être subordonnée au consentement de ces employés. Cependant, si la finalité est de vérifier le respect d'une convention collective ou d'autres conditions de travail et si l'opération est menée par les représentants des employés, ce qui peut être le cas pour certains Etats membres, le transfert de données à caractère personnel liées à des employés non membres de l'organe représentatif peut être effectué si nécessaire pour vérifier ce respect.

59. L'expression « convention collective » s'entend de tout accord conclu entre une organisation d'employeurs ou un employeur, d'une part, et un syndicat, d'autre part. Cet accord doit être écrit et porte normalement sur les conditions d'emploi et sur la relation entre l'employeur et l'employé.

60. Par ailleurs, aux fins de la présente recommandation, le terme « communication » visé aux principes 7 et 8 désigne également la divulgation, la transmission et le transfert de données à caractère personnel.

61. La quantité d'informations personnelles qui peut être communiquée doit satisfaire au principe de la proportionnalité – « uniquement si de telles données sont nécessaires pour permettre [aux représentants] de représenter (…) les intérêts des employés ». Le volume de données qui peut être communiqué aux organes représentatifs dépendra de toute évidence de chaque pays, en particulier de l'existence ou non d'une réglementation officielle des relations entre employeurs et organes représentatifs. Ainsi, la législation nationale peut autoriser la communication de données à caractère personnel sur un candidat à une promotion pour permettre la consultation d'un comité d'entreprise avant toute décision. Les obligations prévues au titre des conventions collectives (voir principe 7.1), concernent habituellement à la fois les employeurs et les employés, et peuvent concerner par exemple les accords salariaux, les conditions d'emploi et les procédures conjointes de règlement des litiges.

62. Les systèmes d'information évoqués au principe 7.2 sont ceux définis au principe 2. Les nouvelles technologies, par exemple les courriers électroniques ou l'intranet, peuvent être utilisées pour communiquer des données sur les employés à leurs représentants. Cette communication devrait se faire conformément à la législation et la pratique nationales. Les accords qui établissent les procédures visant à garantir une utilisation sécurisée des données et la confidentialité des communications devraient également être prévus par le droit interne ou déterminés par les autorités responsables de la protection des données.

63. Il convient d'évoquer ici le vote électronique, souvent en ligne, qui s'est largement développé au cours des dernières années, notamment pour les élections des représentants du personnel dans les entreprises. Ce vote électronique peut présenter des risques pour les employés, notamment un risque de divulgation de données sensibles telles que l'adhésion à un syndicat ou des opinions politiques. Le traitement des données personnelles nécessaires pour le scrutin devrait s'efforcer de protéger la vie privée des employés. La mise en œuvre de mesures de sécurité efficaces est un aspect essentiel du succès de l'élection, telle que l'utilisation de méthodes cryptographiques, de cachets et d'encodage des données.

64. Les données traitées par les organes représentatifs dans ces cas sont naturellement régies par les principes généraux de la protection des données, et cela notamment lors des scrutins électroniques évoqués ci-dessus.

8. Communication externe des données

65. Il a été relevé que l'employeur peut servir d'intermédiaire entre l'Etat et l'employé lorsqu'il est nécessaire de fournir des données aux organismes publics, visés au paragraphe 8.1. Il peut s'agir notamment de

l'administration fiscale ou de la sécurité sociale ou encore des inspections de la santé et de la sécurité. La nature et le volume des données à caractère personnel qui peuvent être communiqués à ces organismes publics seront déterminés dans la mesure où les obligations légales sont satisfaites. L'expression « obligations légales » devrait par conséquent être entendue dans ce sens.

66. Les organismes publics peuvent demander à ce que des données à caractère personnel soient traitées pour leur permettre d'exercer leurs fonctions officielles – par exemple en vue d'une étude publique sur les blessures et les maladies professionnelles ou d'une analyse des formes d'emploi dans les zones défavorisées. Il est reconnu que l'expression « conformément à d'autres dispositions du droit interne » peut obliger à communiquer des données sur les employés dans ces circonstances (pour la définition de « communication », voir paragraphe 56 ci-dessus) et dépend du contexte national. En outre, la législation nationale, conformément à la CEDH, peu parfois nécessiter la communication de données à caractère personnel aux autorités de police, au corps judiciaire, ainsi qu'à d'autres organismes publics dans le cadre de l'exercice de leurs fonctions officielles. Il convient de relever que, dans ces cas, les données à caractère personnel ne sont pas communiquées à des fins d'emploi. Ainsi, les procédures de divorce entre un(e) employé(e) et son époux/se peuvent nécessiter la communication d'informations sur le salaire de l'employé par l'employeur au tribunal pour permettre à ce dernier d'évaluer le montant de la pension alimentaire à verser à la dissolution du mariage. En ce qui concerne la communication de données à caractère personnel aux autorités de police – qui peut être requise par la législation nationale appliquée conformément à la Convention n° 108 – il convient de faire référence également aux dispositions de la Recommandation n° R (87) 15 du Comité des Ministres aux Etats membres visant à réglementer l'utilisation des données à caractère personnel dans le secteur de la police.

67. Le principe 8.2 se rapporte aux situations où les données à caractère personnel doivent être communiquées en dehors du lieu de travail à des organismes publics et ce, en dehors de l'exercice de leurs fonctions officielles – par exemple un organisme public agissant en qualité d'employeur sur le marché du travail –, ainsi qu'à des parties privées, y compris les entités au sein du même groupe.

68. Le principe 8.2.a traite de la communication de données à caractère personnel à des fins d'emploi au type d'organismes cités ci-dessus. Ainsi, un employeur peut recruter un auditeur pour gérer les comptes de la société, payer les salaires, se charger des obligations fiscales des employés, etc.; ou alors un employé peut être temporairement affecté auprès d'un autre employeur. Dans ces deux cas, il est nécessaire de divulguer des données personnelles. Le texte admet que la communication de ces informations est alors légitime, puisque ces aspects entrent dans le champ d'application de l'expression « à des fins d'emploi ». Il convient de noter que la légitimité de la communication de données dans ces cas est subordonnée au respect de la finalité d'origine (« qui ne seraient pas incompatibles avec les finalités pour lesquelles les données ont été collectées à l'origine »), et les considérations prises en compte au principe 6.3 valent également pour l'interprétation du principe 8.2.*a*. Celui-ci subordonne en outre la communication de données à la communication préalable des informations y relatives à l'employé concerné ou à ses représentants. Une fois encore, le texte de la recommandation reconnaît l'importance d'une protection transparente des données.

69. En ce qui concerne le principe 8.2.*b*, les données à caractère personnel qui doivent être communiquées peuvent ne pas être destinées à être utilisées des fins d'emploi (par exemple dans le cadre d'une demande émanant d'une société de marketing direct ou d'un parti politique en vue d'obtenir la liste des noms et adresses des employés). Dans de telles situations, les garanties sont renforcées : le consentement exprès, libre, spécifique et informé de l'employé est nécessaire.

70. Il peut également arriver que le droit interne autorise la communication de données à caractère personnel à des organismes privés ou à des organismes publics en dehors de l'exercice de leurs fonctions officielles. La législation nationale en matière de statistiques en est un exemple. Plus souvent, la communication visée au principe 8.2.*c* est prévue aux fins de s'acquitter d'obligations légales liées, par exemple, à la sécurité et à la protection sociales des employés, ou pour optimiser l'affectation des ressources humaines ou encore, le cas échéant, à des fins judiciaires, notamment l'exercice du droit de recours.

71. Les principes 8.3 et 8.4 ont été introduits à la lumière d'autres législations qui visent à renforcer la transparence des activités des administrations publiques et à faciliter l'accès aux documents publics en introduisant diverses obligations relatives à la publication et à la diffusion, par les administrations publiques, de fichiers, documents et informations sur leur organisation et leurs activités. La communication des données relatives aux effectifs d'un organisme public peut couvrir divers aspects, notamment les noms des employés, les organigrammes et les répertoires internes, ainsi que d'autres données permettant d'identifier les employés, par exemple les informations sur les salaires et les pensions, les indemnités de départ et les accords de compromis, les statistiques relatives aux arrêts maladie et les dossiers de formation.

72. Plusieurs facteurs permettent d'indiquer si la communication est loyale, notamment si elle est nécessaire et proportionnée à la satisfaction de l'intérêt public en jeu, s'il s'agit de données à caractère personnel sensibles, les conséquences de la divulgation de ces informations et la conciliation des droits des employés avec l'intérêt public légitime à divulguer les informations en question. En principe, les informations doivent concerner leur rôle public plutôt que leur vie privée. S'il s'agit de données à caractère personnel

sensibles, l'article 6 de la Convention n° 108 devrait être pleinement respecté. Ces données concernent généralement les aspects les plus personnels de la vie des employés, par exemple leur santé ou leur vie sexuelle, plutôt que leur vie professionnelle.

73. Des garanties complémentaires peuvent être envisagées en matière de loyauté du traitement et de la publication des données relatives aux employés, par exemple la détermination de délais proportionnels pour leur publication et l'adoption de mesures permettant de restreindre la disponibilité de ces informations dans les moteurs de recherche externes.

9. Traitement des données sensibles

74. A l'instar de la Convention n° 108 et d'autres recommandations en matière de protection des données, un paragraphe distinct est consacré à la question des données sensibles. Il est à noter, toutefois, que le principe 9 contient également des lignes directrices spéciales pour le traitement des données relatives à la santé, ces données étant plus courantes dans le secteur de l'emploi que les autres types de données évoqués au principe 9.1. C'est pourquoi les données de santé font l'objet d'une attention plus soutenue. Il convient également de tenir dûment compte de la Recommandation n° R (97) 5 du Comité des Ministres aux Etats membres relative à la protection des données médicales.

75. Une attention particulière devrait être accordée aux technologies médicales qui permettent d'obtenir les informations les plus intimes sur l'état de santé de l'employé. Eu égard aux droits au respect de la vie privée et de la dignité humaine, ces techniques devraient être utilisées avec prudence, uniquement dans les cas prévus par la législation nationale y afférente et sous réserve de garanties appropriées. On peut à cet égard faire référence à la Recommandation n° R (94) 11 du Comité des Ministres aux Etats membres sur le dépistage comme instrument de médecine préventive. Par ailleurs, les employeurs des secteurs public comme privé devraient être informés des dispositions de la Recommandation n° R (87) 25 du Comité des Ministres aux Etats membres concernant une politique européenne commune de santé publique de lutte contre le syndrome d'immunodéficience acquise (sida). Dans cette recommandation, le Comité des Ministres invite à ne pas introduire de dépistage obligatoire pour la population en général, ni pour des groupes particuliers. Il est jugé souhaitable que les employeurs adoptent la même démarche dans le secteur de l'emploi en se gardant d'obliger les candidats à l'emploi à subir un test de dépistage du sida contre leur gré.

76. Les principes énoncés plus haut dans la recommandation en ce qui concerne le traitement des données à caractère personnel doivent être lus à la lumière des dispositions relatives aux données sensibles énoncées à l'article 6 de la Convention n° 108. Ces principes visent à adapter cet article aux exigences du secteur de l'emploi, pour lequel aucune exception n'est envisagée, mis à part celles prévues par le droit interne, par exemple lorsque le traitement est nécessaire pour les besoins des systèmes de retraite ou des régimes d'assurance-maladie négociés par les employeurs et les syndicats, à condition qu'il existe des garanties appropriées. Les garanties supplémentaires devraient être principalement destinées à garantir la sécurité et le traitement licite des données. Pour ce qui est des cas non couverts par cette exception, l'interdiction du traitement des données sensibles demeure la règle ; la dérogation à cette règle est uniquement possible lorsque le droit interne prévoit les garanties appropriées. Par ailleurs, il convient d'attirer l'attention des employeurs sur l'interdiction stricte de collecter des données sensibles qui sont sans rapport avec la nature de l'emploi et risquent d'entraîner une discrimination à l'égard de certains employés, par exemple le rejet de candidats à l'emploi en raison de leurs convictions religieuses ou politiques, ou l'isolement ou le renvoi d'un employé à cause de ses préférences sexuelles.

77. A l'inverse, certains types de données sensibles peuvent être traités de manière licite si la nature même de l'emploi nécessite leur obtention : ainsi, les organisations politiques dont la mission consiste à influencer l'opinion publique ont besoin d'informations sur les opinions politiques des candidats à des postes au sein de leur organisation ; les institutions religieuses demandent aux candidats qui souhaitent travailler pour elles d'indiquer leurs convictions religieuses au moment du recrutement. Cela étant, le traitement de ces données n'est légal que si les garanties spécifiques et complémentaires appropriées sont prévues par le droit interne.

78. Le principe 9.2 énonce les situations dans lesquelles il est probable que des données de santé soient traitées dans le cadre de l'emploi. Il s'agit des données relatives à la santé physique et mentale. Les principes 9.2 et suivants sont structurés de sorte à restreindre le traitement des données relatives à la santé, tout en renforçant la nécessité de sécuriser ces données. En ce qui concerne la collecte, le principe 9.2 prévoit des restrictions quant aux sortes de données de santé qui peuvent être recueillies. Il est à noter que sont concernées les données de santé relatives aux employés mais aussi aux candidats à l'emploi.

79. Le principe 9.2.*a* fait référence à l'aptitude d'un employé à exercer ses fonctions. En vertu de ce principe, les données relatives à la santé peuvent uniquement être obtenues si elles sont nécessaires pour déterminer si l'employé est apte à un emploi particulier, par exemple à participer à une expédition s'il s'agit d'un scientifique. La nécessité du traitement des données de santé doit être évaluée à l'aune de la finalité de chaque cas concret. La référence aux « besoins de la médecine préventive », au principe 9.2.*b*, couvre les bilans périodiques, par exemple pour s'assurer que les employés exposés à des substances toxiques dans le cadre de

leur travail ne développent aucune maladie. Le principe 9.2.*c* autorise la collecte de données sur la santé pour permettre à un employé de travailler dans des conditions adaptées à sa maladie ou à son handicap. Le traitement des données de santé pour des motifs liés à la sauvegarde des intérêts vitaux de la personne concernée ou d'autres employés, comme indiqué au principe 9.2.*d*, concerne généralement les situations d'urgence, lesquelles seront évaluées au cas par cas. Le principe 9.2.*e* autorise la collecte de données sur la santé pour permettre l'octroi de « prestations sociales » à un employé. Ainsi, un employé blessé sur son lieu de travail qui demande une indemnisation au titre d'un contrat d'assurance peut avoir besoin d'être examiné par un médecin pour déterminer la nature et l'étendue de son incapacité. Par ailleurs, les régimes des accidents du travail ou les systèmes d'indemnisation des employés gérés par l'Etat peuvent nécessiter la collecte de données sur l'état de santé d'un employé en vue du règlement d'une demande d'indemnisation ou pour évaluer la probabilité de réclamations futures.

80. La nature de l'emploi détermine bien évidemment le type de questions qui peuvent être posées à un employé ou à un candidat à l'emploi et, partant, le volume de données qui peut être collecté. La nature de l'emploi détermine également celle de l'examen physique. Ainsi, il peut être demandé à un candidat à un emploi dans une centrale nucléaire de fournir des informations sur l'incidence du cancer ou d'autres maladies dans sa famille, outre le fait qu'il doit passer un examen médical exhaustif. Il ne sera pas demandé de même à des candidats à un emploi dans une profession libérale.

81. Le principe 9.3 rappelle que le respect des droits et des libertés fondamentales devrait être garanti au cours de la collecte des données. A cet égard, il interdit aux employeurs de traiter des données génétiques relatives aux employés car il risque d'en découler une discrimination dans tous les aspects de l'emploi. Le traitement des données génétiques peut uniquement être autorisé dans des cas très exceptionnels, réglementés par les dispositions du droit interne. D'après la Recommandation n° R (97) 5, un tel traitement ne peut être permis que pour des raisons de santé et en particulier pour éviter toute atteinte grave à la santé de la personne concernée ou de tiers. Le traitement des données génétiques peut se faire par exemple dans le cadre d'un programme de suivi génétique qui observe les effets biologiques de substances toxiques sur le lieu de travail, lorsqu'un tel programme est imposé par la loi ou, dans des conditions strictement définies, lorsque le programme se fait sur une base volontaire.

82. Il convient d'évoquer la Recommandation n° R (92) 3 du Comité des Ministres aux Etats membres sur les tests et le dépistage génétique à des fins médicales, et en particulier son principe 6, qui prévoit que « (…) l'accès à certaines activités ou la poursuite de leur exercice, en particulier l'emploi, ne doivent pas être subordonnés à une obligation de subir des tests ou un dépistage génétique ». Ce même principe établit par ailleurs que « toute exception à ce principe doit être justifiée par des raisons de protection immédiate de la personne concernée ou d'un tiers et être directement liée aux conditions spécifiques de cette activité ».

83. Le principe 9.4 stipule que l'employeur peut uniquement obtenir des données auprès de l'employé concerné et n'a pas le droit de recueillir des données de santé directement auprès d'autres sources, par exemple en contactant un ancien employeur. L'employé devrait être la source principale d'information aux fins de fournir des informations en matière de santé – en premier lieu par son examen physique et par ses réponses aux questions qui lui sont posées pour déterminer son aptitude à l'emploi, à condition qu'un tel traitement soit légal.

84. Le principe 9.5 porte sur les situations où le personnel tenu au « secret médical » peut avoir accès à des données de santé confidentielles du point de vue médical. Il devrait uniquement s'agir des situations où il est nécessaire de déterminer l'aptitude d'un employé à exercer ses fonctions ou des situations où le traitement des données de santé par l'employeur est nécessaire pour imposer des mesures qui protègent la santé de l'employé ou préviennent les risques pour les autres. Il convient de noter que, aux principes 9.5 et 9.6, les rédacteurs de la recommandation font volontairement la distinction entre les données de santé en général et les données de santé couvertes par le secret médical. Il va sans dire que ces dernières nécessitent une protection particulière.

85. Sous réserve des règles relatives à la collecte de données à caractère personnel couvertes par le secret médical, mentionnées aux principes 9.5 et 9.6, et contrairement aux autres catégories de données sensibles visées au principe 9.1, le traitement des données relatives à la santé des employés ou des candidats à l'emploi n'est pas soumis à une exigence de « cas particuliers ». Il est admis que le traitement de ces données est généralisé et nécessaire dans le secteur de l'emploi. Il revient à la législation interne de déterminer le type de données couvertes par le secret médical.

86. Lorsqu'une entreprise ou une organisation emploie son propre personnel médical pour effectuer les examens médicaux des employés ou des candidats à l'emploi, il est essentiel que ce personnel préserve le secret médical à tous les niveaux, même devant l'employeur. Les employeurs ne devraient pas recevoir d'informations médicales, mais uniquement des conclusions pertinentes pour la décision de recrutement. Les catégories de personnes, autres que les médecins, qui sont tenues au secret médical devraient être déterminées conformément à la législation et à la pratique nationales. Le principe 9.5 prévoit des restrictions importantes en matière de communication de données médicales *stricto sensu* au personnel administratif, étant

entendu que des indications générales sur l'état de santé d'un employé ou d'un candidat à l'emploi peuvent être fournies (X a passé son examen médical ; les résultats de l'examen médical révèlent que Y n'est plus suffisamment apte à poursuivre son travail, etc.). Lorsque des données de santé doivent être communiquées à l'administration du personnel, elles ne peuvent être conservées que par celle-ci, en stricte conformité avec les principes 5 et 6 de la présente recommandation.

87. La confidentialité des données de santé est compromise lorsque ces données sont intégrées à un état de services contenant diverses autres catégories de données. La séparation physique permet également de renforcer la sécurité des données. Il convient de prêter attention à l'utilisation des mots de passe pour l'accès sélectif aux données conservées, de façon à s'assurer que seuls les membres du service médical peuvent y accéder. D'autres moyens techniques peuvent être utilisés pour empêcher les accès non autorisés.

88. Il est reconnu que le traitement des données de santé peut nécessiter la coopération de personnes qui ne travaillent pas au sein du service médical et ne sont pas soumises aux mêmes codes déontologiques, ni aux mêmes exigences en matière de secret médical – par exemple le personnel chargé des technologies de l'information (TI). Ces personnes doivent impérativement être conscientes du caractère sensible des informations qu'elles traitent et de la nécessité de respecter leur nature confidentielle.

89. En ce qui concerne le traitement de données de santé relatives à des tiers (voir principe 9.7), on peut faire référence aux membres de la famille de l'employé visés par l'octroi de prestations particulières.

10. Transparence du traitement

90. Le principe 10 propose plusieurs manières d'informer les employés de leurs droits ainsi que des activités de traitement de données effectuées par l'employeur. Une description particulièrement claire et complète doit être faite du type de données à caractère personnel qui peuvent être collectées au moyen des systèmes et technologies de l'information, par lesquels l'employeur peut les surveiller, et de l'utilisation possible qui peut en être faite. Une politique générale devrait en outre expliquer comment des opérations cachées de surveillance pourraient avoir lieu.

91. Une description similaire devrait être faite de l'utilisation des technologies biométriques et d'identification par radiofréquence (RFID), de l'utilisation possible des codes d'identification personnelle et du rôle du personnel chargé des TI (administrateurs système, par exemple) en relation avec le traitement des données.

92. Les informations devraient également préciser les droits de l'employé en ce qui concerne ses données, conformément au principe 11 de la présente recommandation, ainsi que les voies et moyens d'exercer ces droits. Les informations visées au principe 10.1 devraient être fournies et mises à jour en temps voulu, en tout état de cause avant que l'employé n'exerce effectivement l'activité ou l'action prévue, et être aussi mises à disposition de l'employé au moyen des systèmes d'information habituellement utilisés par lui.

93. A cet égard, il convient de noter que le terme « destinataire », inclus dans le type d'information à communiquer aux employés, désigne toute personne physique ou morale, autorité publique, service, agence ou autre organisme à qui des données sont divulguées ou rendues disponibles.

94. Conformément à la législation ou à la pratique nationales et, le cas échéant, aux conventions collectives pertinentes, les employeurs devraient au préalable informer pleinement ou consulter leurs employés ou leurs représentants quant à l'introduction, l'adaptation et l'utilisation des systèmes et technologies de l'information pour la collecte et l'exploitation des données à caractère personnel nécessaires pour des besoins de production ou de sécurité, ou encore d'organisation du travail.

11. Droit d'accès, de rectification et d'opposition

95. Les employés devraient pouvoir être informés des données à caractère personnel les concernant qui sont traitées. En vertu du principe 11.1, chaque employé qui en fait la demande devrait pouvoir accéder à l'ensemble des données à caractère personnel conservées par l'employeur à son sujet. L'employé devrait également avoir le droit de connaître toutes les informations disponibles sur la source de ces données, les parties à qui elles ont été ou pourraient être communiquées et/ou la logique qui sous-tend tout processus automatisé le concernant. A cette fin, l'employeur devrait mettre en place des procédures générales visant à garantir une réponse appropriée et rapide lorsque le droit d'accès, d'effacement et de rectification est exercé, en particulier dans les grandes entités ou les entités dispersées sur le territoire national.

96. L'expression « responsable du traitement », figurant au principe 11.1, désigne la personne ou l'organisme habilité(e) à prendre des décisions quant au traitement des données, que cette compétence découle de dispositions juridiques ou de circonstances de fait. Dans certains cas, il peut y avoir plusieurs responsables ou des coresponsables (responsables conjointement d'un traitement et, éventuellement, responsables d'aspects différents de ce traitement). Au titre des principes énoncés dans la présente recommandation, le responsable du traitement est généralement l'employeur. Le « sous-traitant », évoqué au principe 20.1, est une entité distincte

agissant pour le compte du responsable et effectuant le traitement de la manière requise par le responsable et pour les besoins de ce dernier. Un employé du responsable n'est pas un sous-traitant, mais une personne concernée, s'agissant du traitement de ses données à caractère personnel.

97. En vertu du principe 11.2, chaque employé devrait avoir le droit d'obtenir la rectification, le blocage ou l'effacement de ses données à caractère personnel lorsque celles-ci sont détenues contrairement à la loi ou aux principes établis dans cette recommandation, notamment lorsqu'elles sont inexactes. La loi peut restreindre le droit de faire opposition, par exemple lorsque le traitement de ces données répond à des exigences posées par la législation fiscale, de la sécurité sociale ou de la sécurité industrielle. Le droit de faire opposition peut ne pas être applicable si le traitement est nécessaire à des fins d'emploi, par exemple pour l'exécution du contrat de travail.

98. Le droit d'accès devrait également être garanti en ce qui concerne les données d'évaluation personnelle (voir principe 11.3), y compris celles relatives aux appréciations de la productivité ou du potentiel de l'employé (voir paragraphe 5.5), au plus tard lorsque le processus d'appréciation est terminé, sans préjudice du droit de défense des employeurs ou des tiers concernés. Le principe 11.3 cherche à instaurer un juste équilibre entre le droit d'accès de l'employé, qui s'étend également aux données d'évaluation, et la nécessité légitime de l'employeur d'évaluer l'employé. Par ailleurs, l'employé devrait disposer d'une voie de recours pour contester l'évaluation et se défendre face à toute évaluation négative, de préférence avant la clôture de celle-ci. Tout report à des fins de défense ne peut être que temporaire.

99. Le principe 11.4 reconnaît le droit, pour un employé, de voir son point de vue pris en compte lorsqu'il fait l'objet d'une décision fondée uniquement sur un traitement automatisé de données ayant une incidence négative (par exemple une mesure disciplinaire, un licenciement, un refus de promotion). Cela peut être le cas par exemple lorsqu'un employé est renvoyé pour non-exécution de ses fonctions sur la base d'un enregistrement de vidéosurveillance, sous réserve que cette mesure de surveillance soit autorisée par la loi, et que la décision de licenciement se fonde uniquement sur les images enregistrées. En outre, le fait qu'une décision se fonde sur un traitement automatisé ne saurait priver l'employé du droit de connaître les motifs de la décision le concernant.

100. Le principe 11.5 est relié au précédent puisque la mise en œuvre des exigences du principe 11.4 exige que l'employé soit informé du raisonnement qui sous-tend la décision automatisée ; à cette fin, l'employé devrait avoir le droit de consulter et d'examiner le raisonnement en question.

101. Le principe 11.6 définit les dérogations possibles aux principes 10, 11.1, 11.2, 11.4 et 11.5. Les droits de l'employé ne sont pas absolus et doivent être conciliés avec d'autres droits et intérêts légitimes. Ils peuvent, conformément à la Convention n° 108, être restreints uniquement lorsque la loi le prévoit et que cette restriction est nécessaire dans une société démocratique dans l'intérêt de motifs légitimes énumérés de manière exhaustive par la Convention. Ainsi, le droit d'être informé du raisonnement qui sous-tend le traitement de données peut être restreint en vue de protéger les droits d'autres personnes, à l'instar des informations confidentielles protégées par le droit (secret commercial, par exemple). En ce qui concerne le droit d'opposition, l'employeur peut avoir un motif légitime impérieux d'effectuer le traitement qui l'emporte sur les intérêts ou les droits et libertés de l'employé. La preuve de cet intérêt légitime doit, à l'évidence, être apportée au cas par cas pour pouvoir poursuivre le traitement. Par ailleurs, il peut exister des limitations pratiques à l'exercice du droit d'accès. Ainsi, un fichier de données particulier peut contenir des données sur plusieurs employés. Dans un tel cas, l'employeur déduit par extrapolation les données personnelles relatives à l'employé concerné et, lorsqu''il n'est pas possible de séparer les données de l'employé qui sollicite l'accès de celles de ses collègues, l'employeur peut être obligé de demander à ces derniers leur consentement avant de pouvoir autoriser l'accès à ce fichier spécifique.

102. La restriction de l'exercice des droits énoncée au principe 11.7 s'applique, par exemple, aux cas où une enquête est ouverte par un employeur après un vol de biens dans une usine ou à des employés. Il convient de noter que, si l'exercice du droit d'accès a été suspendu – ce qui ne peut se faire que dans la mesure indispensable aux besoins de l'enquête – cette suspension ne saurait durer une fois l'enquête close.

103. La personne désignée par l'employé conformément aux dispositions du principe 11.8 peut être un collègue, un avocat ou son représentant. Ce qui est essentiel, c'est que l'employé lui-même doit désigner cette personne. Le principe 11.8 admet que le droit interne puisse restreindre, voire interdire, l'assistance à un employé.

104. Le droit interne déterminera plus avant la nature des voies de recours évoquées au principe 11.9. Ces voies de recours présupposent l'intervention d'une autorité indépendante, qu'il s'agisse d'un tribunal ou d'un organe indépendant au sens du protocole additionnel à la Convention n° 108, c'est-à-dire doté de pouvoirs d'investigation et habilité à ordonner des sanctions appropriées.

12. Sécurité des données

105. Le principe 12.1 porte sur les mesures techniques et organisationnelles qui devraient être prises pour garantir la sécurité des données. Si cette recommandation peut être mise en œuvre par voie juridique, d'autres moyens peuvent aussi être envisagés, notamment l'établissement de politiques et de procédures internes en matière de sécurité. Des précautions pratiques doivent également être prises par le responsable du traitement pour éviter tout incident de traitement accidentel ou malveillant. Le niveau de sécurité doit être approprié à la probabilité et à la gravité des risques posés par le traitement des données, et à la nature des données à caractère personnel, ainsi qu'à la nature, à la portée, au contexte et à la finalité du traitement.

106. Les mesures techniques et organisationnelles appropriées, évoquées au principe 12.1, devraient être adaptées à chaque situation et assurer ainsi une protection effective des données. Il pourrait s'agir par exemple :

a. d'inventaires à jour des opérations de traitement ;
b. d'études d'impact sur la vie privée pour les opérations de traitement qui présentent un risque élevé ;
c. de la nomination d'une personne chargée de la protection des données ou d'une attribution plus précise des responsabilités en vue de garantir une gestion plus structurée du traitement des données ; l'introduction de mécanismes d'audit interne ou d'inspection indépendante de l'état d'avancement de la mise en œuvre de la législation ;
d. de l'établissement de procédures internes visant à mettre en lumière les risques pour la sécurité ou les atteintes en la matière ;
e. des activités de formation et la certification à différents niveaux, notamment celui de l'encadrement.

En outre, il convient de rappeler que la minimisation des données présente des avantages en termes de prévention dès le début du traitement. De même, en cas de violation des données, l'employeur devrait mettre en œuvre les mesures technologiques de protection appropriées pour prévenir toute atteinte aux droits des employés et informer dans les meilleurs délais les employés concernés par cette violation.

107. Le principe 12 concerne non seulement les employeurs, mais aussi les tiers, tels que les agences pour l'emploi et les sociétés de TI qui traitent les données à caractère personnel relatives aux employés pour le compte des employeurs (« entités auprès desquelles le traitement de données peut être sous-traité »). On renverra à cet égard aux obligations du « sous-traitant », qui est une entité distincte agissant pour le compte du responsable du traitement et effectuant le traitement de données de la manière requise par le responsable du traitement et pour les besoins de celui-ci (voir également paragraphe 90). Les règles relatives à la sécurité du traitement de données supposent l'obligation, pour le responsable du traitement et le sous-traitant, de prendre des mesures techniques et organisationnelles appropriées afin de prévenir toute intervention non autorisée dans les opérations de traitement des données [voir Directive 95/46/EC].

108. Le principe 12.3 énonce les obligations qui incombent à l'administration du personnel ainsi qu'aux autres personnes intervenant dans le traitement des données (webmasters, etc.), qui, dans l'exercice de leurs fonctions liées au fonctionnement normal et à la sécurité des réseaux, ont accès à un certain volume de données à caractère personnel par le biais des boîtes électroniques, des fichiers de connexion, des fichiers temporaires ou des cookies. En vertu de ce principe, l'employeur doit informer le personnel qui participe au traitement des données des mesures de sécurité qu'il est tenu d'appliquer, de préférence au moyen de règles internes. Une autre mesure consisterait à insérer une clause de confidentialité dans leur contrat de travail et, le cas échéant, dans la charte informatique de l'établissement ou dans le règlement intérieur.

13. Conservation des données

109. En vertu du principe 13.1, la période pendant laquelle des données à caractère personnel peuvent être conservées par un employeur devrait être déterminée selon les finalités d'emploi définies au principe 2 de la recommandation. Pour certaines finalités d'emploi, le temps de conservation nécessaire sera plus long que pour d'autres finalités d'emploi. La durée de conservation des données sera déterminée au cas par cas. Par exemple, le versement de prestations de retraite au titre d'un régime d'entreprise obligera l'employeur à conserver des données bien après la retraite de l'employé.

110. Le principe 13.2 accorde une attention particulière aux données à caractère personnel fournies par les candidats à l'emploi. En principe, ces données devraient être effacées dès lors que la candidature est rejetée. En outre, les documents fournis par le candidat devraient soit lui être retournés, soit être supprimés du système (lorsque les candidatures se font en ligne, par exemple). Cela étant, il peut arriver qu'un employeur souhaite conserver des informations sur un candidat particulier qui n'a peut-être pas rempli les conditions requises pour l'emploi en question, mais qui pourrait être retenu à un stade ultérieur pour un autre poste pour lequel il convient mieux. Le candidat rejeté peut également avoir intérêt à ce que les informations le concernant soient conservées dans les bases de données de l'employeur. Néanmoins, l'employeur devrait alors au préalable en informer dûment le candidat à l'emploi et obtenir son consentement.

111. Le principe 13.3 envisage également la possibilité, pour l'employeur, de conserver des données fournies à la suite d'un acte de candidature à titre de précaution contre une éventuelle action en justice intentée par un

candidat rejeté ou à d'autres fins légitimes. Ainsi, l'employeur peut souhaiter apporter la preuve à un tribunal que la candidature n'a pas été rejetée pour des motifs liés au sexe, à la religion, etc., ou que les procédures appropriées en matière de recrutement et d'entretien ont été appliquées. Dans ce cas, les données devraient être conservées uniquement pendant le temps nécessaire à l'atteinte de cette finalité, avant d'être effacées une fois expirée la période prescrite pour engager une procédure judiciaire. Au besoin, les données fournies devraient également être conservées, si nécessaire, à d'autres fins légitimes. Ce peut être le cas lorsqu'un employeur est légalement tenu de fournir des informations sur des aspects de leurs activités qui peuvent s'avérer importants pour contrôler l'application d'une loi, par exemple la législation anti-discrimination. Dans un tel cas, les données devraient être conservées aussi longtemps que nécessaire.

112. D'après le principe 13.4, lorsqu'une enquête interne est menée et qu'elle n'entraîne aucune poursuite ou mesure négative à l'encontre de l'employé concerné, les données devraient être effacées à l'issue d'une période raisonnable. Aucune règle n'est précisée quant à ce qui constitue une période raisonnable. Comme indiqué plus haut, la période pendant laquelle les données sont conservées est à déterminer au cas par cas. Une attention particulière doit être accordée au droit d'accès de l'employé concerné. Si l'exercice de ce droit a été suspendu pour les besoins de l'enquête, les données à caractère personnel traitées aux fins de cette enquête devraient être communiquées à l'employé concerné avant leur suppression.

Partie II – Formes particulières de traitement

14. Utilisation de l'internet et des communications électroniques sur le lieu de travail

113. Les employeurs ont le droit d'encourager une gestion efficace et de se protéger contre les obligations et dommages-intérêts qui pourraient découler d'une action en justice intentée par des employés. Les activités de contrôle et de surveillance menées dans l'intérêt de l'employeur devraient toutefois être licites, transparentes, efficaces et proportionnées – une approche raisonnable qui permet également d'éviter les effets négatifs éventuels sur la qualité de la relation professionnelle.

114. Pour empêcher toute atteinte injustifiable aux droits au respect de la vie privée et à la protection des données à caractère personnel dans le cadre d'un éventuel traitement de ces données en relation avec l'utilisation de l'internet ou de l'intranet, les employeurs pourraient avoir à communiquer de manière formelle les informations aux personnes concernées (voir principe 16.1) dans un document, tel qu'une charte informatique ou une politique relative à la vie privée, qui devrait être signé par les employés et régulièrement mis à jour. Les informations contenues dans la politique relative à l'utilisation des moyens de communication et à la surveillance devraient être claires, exhaustives, exactes et facilement accessibles.

115. Le principe 14.1 s'applique à tous les aspects de l'emploi d'un employé, y compris l'utilisation d'ordinateurs, de smartphones ou de dispositifs numériques, que ce soit dans le cadre de l'utilisation des services intranet ou extranet mis en place par l'employeur, ou de l'utilisation directe ou indirecte de l'internet fourni par l'employeur. Peu importe si le dispositif utilisé par l'employé est fourni par l'employeur ou l'employé lui-même[6]. Par ailleurs, il arrive souvent que les appareils informatiques installés sur le lieu de travail soient utilisés à des fins autres que professionnelles. Même si cette utilisation doit rester appropriée et loyale, et qu'elle ne doit compromettre ni la sécurité des réseaux, ni la productivité de l'établissement, l'employeur peut déterminer les conditions et restrictions en matière d'utilisation de l'internet ne constituant pas une violation disproportionnée de la vie privée des employés.

116. Le principe 14.2 porte sur le traitement de données à caractère personnel relatives aux pages internet or intranet consultées par l'employé. En vertu de ce principe, l'employeur peut adopter des mesures appropriées pour réduire le risque d'utilisation impropre de l'internet (consultation de sites non pertinents, téléchargement par réception ou transmission de fichiers ou de logiciels, utilisation des réseaux pour des finalités non liées au travail), même en utilisant des filtres, évitant ainsi le traitement ultérieur de données à caractère personnel relatives aux employés qui pourraient de surcroît comporter des données sensibles.

117. L'employeur pourrait notamment prendre les mesures suivantes :

a. identifier a priori et indiquer précisément les catégories de sites qui n'ont assurément aucun rapport avec le travail ;
b. veiller à ce que, le cas échéant, dans le cadre des examens/bilans, seules les données anonymes ou celles qui ne permettent pas d'identifier directement les utilisateurs soient traitées au moyen de techniques d'agrégation des données appropriées (par exemple l'analyse des fichiers journaux liés aux connexions à l'internet par des groupes d'employés uniquement).

118. Le principe 14.3 énonce les conditions dans lesquelles l'accès aux communications électroniques professionnelles des employés est légal. Il convient de noter que, aux fins de la recommandation, l'expression « communications professionnelles » désigne notamment les courriers électroniques envoyés ou reçus dans le cadre de l'exercice des fonctions de l'employé, ou les informations professionnelles échangées par le biais des services de messagerie internet. L'accès aux communications électroniques professionnelles peut, par exemple, être nécessaire pour obtenir une confirmation ou une preuve de comportement répréhensible, ou pour détecter des atteintes à la propriété intellectuelle de l'employeur. Lorsqu'il existe une nécessité professionnelle d'accéder à ces communications, les employeurs devraient apporter la preuve des besoins en matière de sécurité ou d'autres raisons légitimes (par exemple lorsque l'employeur est tenu responsable des actions de ses employés, qu'il doit détecter la présence de virus ou garantir la sécurité du système d'information). Les employeurs devraient par ailleurs prendre les mesures nécessaires et prévoir des procédures appropriées afin de pouvoir accéder aux communications électroniques professionnelles d'un employé. A titre d'exemple, si un employé s'absente à l'improviste et/ou pour une période prolongée et si l'employeur a besoin d'accéder aux contenus de ses courriers électroniques pour répondre à des exigences professionnelles urgentes, l'employé en question devrait pouvoir charger un de ses collègues (tiers de confiance) de vérifier les contenus de ses courriers électroniques et de transférer les messages à caractère professionnel à l'employeur.

119. Outre la nécessité de justifier par des motifs légitimes impérieux l'accès aux communications électroniques professionnelles d'un employé, l'employeur doit en outre informer au préalable les employés de l'existence de cette possibilité, de préférence au moyen d'une politique interne explicite. Pour être appropriée,

[6] Voir les lignes directrices sur l'apport de son propre ordinateur portable et de ses outils de communication au travail, en anglais « Bring Your Own Device » (BYOD), Bureau du Commissaire à l'information (ICO)
http://ico.org.uk/for_organisations/data_protection/topic_guides/online/byod

cette politique doit préciser clairement les attentes légitimes des employés ou des tiers en matière de confidentialité de leurs communications.

120. Il peut parfois arriver qu'il soit difficile de distinguer une communication professionnelle d'une communication personnelle. Dans certains pays, le contenu des communications électroniques – ainsi que certaines données extérieures à ces communications et les fichiers joints – est protégé par une garantie de la confidentialité de la correspondance et de la communication, qui est parfois consacrée dans le droit constitutionnel. Au moins au début, l'accès devrait en principe être restreint aux données relatives à la communication (durée, destinataire, etc.) plutôt qu'au contenu même de la communication, si cela est suffisant pour répondre aux besoins de l'employeur.

121. Le principe 14.4 stipule que les communications privées au travail ne doivent pas être surveillées, qu'il s'agisse de leur contenu ou des informations sur leur envoi ou leur réception.

122. Le principe 14.5 porte sur les situations où l'employé quitte l'organisation. Il indique que les employeurs doivent désactiver le compte de l'ancien employé de sorte à ne pas avoir accès à ses communications après son départ. Si l'employeur souhaite récupérer le contenu du compte de l'employé, il doit prendre les mesures nécessaires pour le faire avant le départ de ce dernier et de préférence en sa présence.

123. Enfin, les principes 14.1 à 14.5 doivent être interprétés au sens où toute immixtion dans les communications privées doit respecter l'article 8 de la CEDH et la jurisprudence correspondante de la Cour.

15. Systèmes et technologies de l'information pour le contrôle des employés, notamment la vidéosurveillance

124. Le principe 15.1 fixe des conditions strictes en ce qui concerne l'introduction et l'utilisation des systèmes et technologies de l'information à des fins de contrôle de l'activité et du comportement des employés. Sans préjudice des mesures relatives à des procédures de défense fondées, l'utilisation de systèmes et technologies de l'information, tels que la vidéosurveillance au travail ou les systèmes de géolocalisation, doit être limitée aux seules nécessités liées à l'organisation et/ou à la production, ou à des fins de sécurité ou de protection de la santé. Ces systèmes ne devraient être autorisés que s'ils sont légitimes, nécessaires, proportionnés, loyaux, transparents et réglementés. Ils ne devraient pas viser à contrôler de manière permanente la qualité et la quantité de travail effectuées par chaque employé, ni à surveiller à distance le comportement ou la localisation des employés.

Par ailleurs, en ce qui concerne les systèmes de vidéosurveillance, les employeurs devraient adopter des mesures préventives, par exemple :

- une période maximale de conservation des données la plus courte possible, à définir et à prévoir dans le système ;
- l'accès et la consultation des images uniquement par des personnes dûment habilitées à le faire, dans le cadre de l'exercice de leurs fonctions (par exemple la personne responsable de la sécurité au sein de l'établissement).

125. Le principe 15.2 indique que le traitement des données à caractère personnel, en relation avec l'utilisation des systèmes et technologies de l'information, doit respecter les libertés et droits fondamentaux de l'employé, en particulier le droit au respect de la vie privée. Ce positionnement concorde avec celui de la Cour, qui a maintes fois répété qu'une vigilance accrue en matière de protection de la vie privée est nécessaire face aux nouvelles technologies de la communication, lesquelles permettent d'enregistrer et de reproduire des données à caractère personnel. En ce qui concerne les systèmes de vidéosurveillance, il est clairement énoncé au principe 15.2 que le placement de caméras dans des endroits tels que les toilettes ou les vestiaires (« endroits tenant à la vie intime des employés ») n'est en aucun cas autorisé.

126. Tout en rappelant que les systèmes de vidéosurveillance entrent dans la catégorie des systèmes et technologies de l'information, le « Rapport contenant des principes directeurs pour la protection des personnes par rapport à la collecte et au traitement de données au moyen de la vidéo-surveillance », adopté par le Comité européen de coopération juridique (CDCJ) du Conseil de l'Europe en mai 2003, indique que « [t]oute activité de vidéo-surveillance suppose de prendre les mesures nécessaires pour veiller à ce que cette activité soit conforme aux principes en matière de protection des données à caractère personnel, notamment : […] de n'utiliser de vidéo-surveillance que si, selon les circonstances, la finalité de cette dernière ne peut être atteinte par d'autres mesures portant moins atteinte au respect de la vie privée ; dans la mesure où celles-ci n'entraînent pas des coûts disproportionnés [… et] d'éviter que les données collectées ne soient indexées, comparées ou conservées sans nécessité. Dans les cas où il s'avère nécessaire de conserver les données, de veiller à ce qu'elles soient effacées dès qu'elles ne sont plus utiles à la finalité déterminée et spécifique recherchée […] ».

127. Le principe 15.3 stipule, en cas de litige ou d'action en justice, que les employés devraient pouvoir se fonder sur les enregistrements réalisés. Néanmoins, l'application de ce principe ne devrait pas entraîner la

conservation des enregistrements réalisés pour une période illimitée et disproportionnée, et les propositions énoncées au principe 3 en matière de protection des données devraient s'appliquer en conséquence.

16. Appareils permettant de localiser les employés

128. Le principe 16.1 concerne l'utilisation d'appareils permettant de localiser un employé et de suivre ses déplacements. Il peut notamment s'agir des technologies d'identification par radiofréquence (« technologies RFID »), du GPS (*Global positioning system*) ou d'appareils portables placés à l'intérieur d'objets, de vêtements ou d'uniformes. Les considérations exposées au principe 15.1 valent également pour l'interprétation du principe 16.1, restreignant l'utilisation de ces appareils aux seules nécessités d'organisation ou à des fins de sécurité et de sûreté, ou encore de protection de la santé, conformément aux principes de proportionnalité et de légitimité, et à condition que leur introduction ne permette pas d'instaurer un contrôle permanent des employés concernés.

129. L'utilisation de ces appareils peut porter atteinte aux droits et libertés des employés, et ne devrait pas entraîner de contrôle permanent de l'employé. Des mesures préventives doivent être envisagées, par exemple la possibilité d'interrompre la géolocalisation en dehors des horaires de travail.

130. Par ailleurs, en ce qui concerne la mise en œuvre du principe 16.1, l'utilisation de ces appareils ne doit permettre ni le traitement de données relatives à certaines infractions (vitesse excessive, par exemple), ni la géolocalisation d'autres personnes.

131. Dans ce contexte, une description particulièrement claire et complète doit être fournie aux employés concernés avant d'utiliser des appareils qui révèlent leur emplacement. Cette notification devrait au minimum informer les employés du type de données à caractère personnel qui peuvent être recueillies au moyen de ces appareils, de leur utilisation possible et également du rôle de tout administrateur de système en relation avec le traitement des données. Cette notification relative à la politique en matière de surveillance doit également valoir pour les autres formes particulières de traitement visées dans la partie II de la présente recommandation.

17. Mécanismes internes de signalement

132. Il s'agit, par exemple, des numéros d'urgence, des adresses électroniques spéciales ou des dispositifs en ligne permettant aux employés de donner l'alerte sur des activités illicites. La Recommandation CM/Rec(2014)7 du Comité des Ministres aux Etats membres sur la protection des lanceurs d'alerte ainsi que l'Avis 1/2006 du Groupe de travail « article 29 » sur la protection des données[7], relatif à l'application des règles de l'Union européenne en matière de protection des données aux mécanismes internes de dénonciation des dysfonctionnements dans les domaines de la comptabilité, des contrôles comptables internes, de l'audit, de la lutte contre la corruption et la criminalité bancaire et financière peuvent apporter des orientations supplémentaires en la matière. L'expression « lanceur d'alerte » désigne généralement une personne qui signale ou révèle un comportement répréhensible ou une activité présumée malhonnête ou illicite au sein d'une organisation, dans le cadre d'une relation de travail, qu'il s'agisse du secteur public ou du secteur privé.

133. Le principe 17 souligne l'importance de la sécurité des données et de la détermination des finalités. Il indique en effet que des mesures de sécurité appropriées doivent être mises en place par l'employeur et que les données à caractère personnel doivent être traitées aux fins du mécanisme interne de signalement relatif au dit signalement ainsi qu'aux fins de respecter les obligations légales découlant du droit interne ou d'une action en justice intentée sur la base du signalement interne.

134. Les personnes concernées par le signalement interne devraient être dûment informées de l'utilisation de leurs données pour pouvoir exercer leurs droits visés au paragraphe 11.

135. Même si le signalement anonyme est possible, d'autres mécanistes devraient lui être préférés afin de protéger les droits et intérêts de toutes les parties concernées, la confidentialité étant la règle en toutes circonstances.

18. Données biométriques

136. Le principe 18 porte sur le traitement des données biométriques à des fins d'emploi. En relation avec les technologies de l'information, la biométrie désigne généralement les technologies qui permettent de mesurer et d'analyser les caractéristiques du corps humain telles que les empreintes digitales, la rétine, l'iris, les intonations de la voix, les traits du visage et la morphologie de la main, en particulier à des fins de vérification de l'identité.

[7] Le Groupe de travail « article 29 » sur la protection des données est un organe consultatif établi en vertu de la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

L'application de la biométrie soulève d'importantes questions en matière de droits de l'homme, car elle touche à l'intégrité du corps humain et à la dignité humaine[8].

137. Comme indiqué au principe 18.1, le traitement de données biométriques visant à identifier ou à vérifier l'identité des employés ne devrait en principe être autorisé que s'il est nécessaire à la protection des intérêts légitimes de l'employeur, des employés ou de tiers, sous réserve que ces intérêts n'empiètent pas sur les droits fondamentaux des employés. L'intérêt légitime peut prévaloir, par exemple, lorsqu'il s'agit de protéger les intérêts vitaux des employés ou lorsqu'il est nécessaire de contrôler l'accès à des zones particulièrement sensibles au plan de la sécurité, telles qu'une centrale nucléaire ou une base militaire.

138. Si l'application de la biométrie est possible dans certaines circonstances, les employeurs devraient utiliser des moyens moins intrusifs, c'est-à-dire des méthodes qui respectent les libertés et droits fondamentaux des personnes, et en particulier le droit au respect de la vie privée et de la dignité humaine.

139. Lorsque l'utilisation de données biométriques est autorisée au titre du principe 18.1, l'accès à ces données est soumis à des exigences de sécurité et de proportionnalité. Les données biométriques ne devraient pas être conservées dans une base de données centralisée et, le cas échéant, la préférence devrait être accordée aux systèmes d'identification et d'authentification biométriques qui s'appuient sur des supports mis à la seule disposition de la personne concernée, permettant ainsi aux employés de conserver eux-mêmes leurs données, sur une carte par exemple.

19. Tests psychologiques, analyses et procédures analogues

140. Les tests psychologiques servent généralement à déterminer, notamment, l'aptitude d'un employé à travailler dans des conditions de stress et à évaluer la mesure dans laquelle un candidat à l'emploi est capable de s'acquitter de ses fonctions efficacement dans de telles conditions.

141. En vertu du principe 19.1, le recours à des tests psychologiques, à des analyses et à des procédures analogues ne devrait être permis que s'il est légitime et nécessaire au regard de l'emploi et que le droit interne prévoit des garanties appropriées. A cet égard, les décisions fondées uniquement sur les résultats de ces tests, analyses et procédures analogues devraient pouvoir être contestées. Les tests psychologiques devraient être effectués par une organisation professionnelle ou un psychologue, exerçant selon des codes déontologiques ou tenus de respecter le secret médical. Le profil individuel ne devrait en aucun cas révéler des informations sur la santé de la personne concernée.

142. Le principe 19.2 prévoit en outre que l'employé ou le candidat à l'emploi concerné doit être informé au préalable des modalités d'utilisation des résultats de ces tests, ainsi que du contenu de ces résultats.

20. Autres traitements de nature à présenter des risques spécifiques au regard des droits des employés

143. En matière de traitement de données, l'informatique en nuage, par exemple, représente un risque particulier pour les droits des employés. Lorsque des organismes publics et des entreprises privées font appel à un fournisseur de services d'informatique dématérialisée, les données sont conservées ou traitées par ce fournisseur et/ou ses sous-traitants. Dans ce cas, les employés risquent de perdre le contrôle de leurs données à caractère personnel et de manquer d'informations quant à la manière dont leurs données sont traitées/sous-traitées, où et par qui. Des préoccupations similaires concernant les droits à la protection des données relatives aux employés peuvent surgir lorsque des appareils portables sont utilisés dans le cadre du travail. Les fonctionnalités de ces appareils, permettant par exemple d'enregistrer les activités des employés, de les suivre ou d'éteindre les appareils à distance, supposent nécessairement un accès aux données à caractère personnel conservées dans ces appareils et un traitement de ces données par l'employeur.

[8] Voir également le Rapport d'étape sur l'application des principes de la Convention n° 108 à la collecte et au traitement des données biométriques (2005), élaboré par le Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD).

144. Le principe 20.1 s'inspire du principe 12 de la recommandation en matière de sécurité des données. Avant d'effectuer le traitement des données, l'employeur et, le cas échéant, le sous-traitant, doivent analyser son impact potentiel sur les libertés et droits fondamentaux des personnes concernées. Cette analyse doit aussi tenir compte du principe de la proportionnalité et se baser sur un examen complet du traitement (c'est-à-dire, l'ensemble des descriptions et documents relatifs aux opérations de traitement, indiquant quelles données à caractère personnel seront traitées et à quelles fins, comment elles seront recueillies, comment elles seront utilisées, les flux de données internes, les divulgations de ces données, les mesures de sécurité, etc.). Pour analyser les risques, il peut être précieux de solliciter l'aide de développeurs de systèmes informatiques, notamment des professionnels de la sécurité, ou de concepteurs, ainsi que d'utilisateurs et d'experts juridiques, ce qui peut permettre de réduire la charge administrative liée à un tel exercice.

145. Afin de minimiser les risques, les employeurs pourraient par exemple former le personnel chargé du traitement des données à caractère personnel, instaurer des procédures de notification appropriées (par exemple, pour indiquer la date à laquelle les données seront supprimées du système), établir des dispositions contractuelles spécifiques lorsque le traitement est sous-traité et mettre en place des procédures internes permettant la vérification et la démonstration de la conformité. Pour effectuer cette vérification et cette démonstration, l'employeur peut notamment désigner une personne responsable de la protection des données, à la disposition de laquelle sont mis tous les moyens nécessaires à l'accomplissement de sa mission de manière indépendante. Cette personne chargée de la protection des données, dont la désignation devrait être notifiée à l'autorité de contrôle, peut appartenir ou non à l'entité du responsable du traitement.

146. En vertu du principe 20.2, les représentants des employés doivent être consultés avant la réalisation d'opérations de traitement présentant un risque élevé, à moins que d'autres garanties ne soient prévues par le droit interne.

21. Garanties complémentaires

147. Le principe 21 vise à souligner les obligations des employeurs qui recourent à des formes particulières de traitement, en particulier celles qui sont susceptibles d'entraîner un contrôle des employés.

148. En ce qui concerne l'obligation d'informer préalablement les employés de l'introduction de systèmes et technologies de l'information permettant le contrôle de leur activité, l'employeur doit indiquer en des termes clairs et précis la manière dont les outils mis à leur disposition seront utilisés et si un contrôle sera effectué, et, dans l'affirmative, quels indicateurs et méthodes seront utilisés.

149. Les informations relatives à la politique en matière d'utilisation et de contrôle des moyens de communication doivent être claires, exhaustives, exactes et facilement accessibles.

150. L'employeur devrait par exemple préciser, le cas échéant :

a. les règles internes relatives à la sécurité des données et des systèmes ou à la protection du secret professionnel, prévues pour toutes les catégories d'employés, ainsi que le rôle de l'administrateur système et toute délocalisation des serveurs dans d'autres pays ;
b. toute utilisation personnelle des outils de communication électronique qui est autorisée et facturée à la partie concernée ou qui est strictement interdite (par exemple le téléchargement ou la possession de logiciels ou de fichiers n'ayant absolument aucun rapport avec l'activité professionnelle), en indiquant également les conséquences possibles, de préférence proportionnelles à la gravité de l'infraction (compte tenu également de la possibilité de consultations involontaires de sites internet découlant d'activités imprévues des moteurs de recherche, des publicités ou des erreurs de frappe) ;
c. tout contrôle que l'employeur se réserve le droit d'effectuer, en indiquant les raisons légitimes et les méthodes utilisées ;
d. les fichiers journaux, s'ils sont conservés, sous la forme également des copies de sauvegarde, et les personnes qui peuvent y accéder.

151. Les employés ou leurs représentants devraient être informés et consultés préalablement à l'introduction ou l'adaptation d'un système de surveillance. Lorsque la procédure de consultation révèle une possibilité d'atteinte au droit au respect de la vie privée et de la dignité humaine d'un employé, l'accord de celui-ci doit être obtenu.

152. Lorsque les employés ne sont pas représentés, d'autres entités spécifiques devraient intervenir pour veiller à ce que ces formes particulières de traitement soient effectuées moyennant les garanties appropriées pour les employés.

153. Une autre garantie opportune pourrait consister à effectuer ne analyse des risques avant d'envisager la réalisation d'une nouvelle opération de traitement.