Exposé des motifs

Recommandation No.R (90) 19 du Comité des Ministres aux Etats membres sur la protection des données à caractère personnel utilisées à des fins de paiement et autres opérations connexes

(adoptée par le Comité des Ministres le 13 septembre 1990, lors de la 443e réunion des Délégués des Ministres)

INTRODUCTION

1. L'impact de la technologie de l'informatique sur les diverses activités des secteurs public et privé a depuis longtemps retenu l'attention du Comité d'experts sur la protection des données du Conseil de l'Europe (CJ-PD), organe intergouvernemental responsable de l'élaboration du seul instrument juridique mondial contraignant dans le domaine de la protection des données - la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 (1). En se concentrant sur des contextes spécifiques de traitement des données, le Comité d'experts a prévu des principes et lignes directrices détaillés sur la protection de la vie privée, fondés sur les dispositions de la Convention mais adaptés concrètement à ces contextes.

2. Les lignes directrices et principes ont donné naissance à des recommandations adoptées par le Comité des Ministres sur la base de projets préparés par le Comité d'experts et ses groupes de travail. Ces recommandations sont adressées par le Comité des Ministres aux gouvernements des Etats membres, les invitant à tenir compte des solutions proposées dans les recommandations lorsqu'ils traitent des questions de protection des données couvertes par ces recommandations.

3. Six initiatives de ce genre ont, jusqu'à présent, été prises dans le cadre de ce que l'on appelle communément une "approche sectorielle" à la protection des données.

- La Recommandation n° R (81) 1 relative à la réglementation applicable aux banques de données médicales automatisées (23 janvier 1981);
- 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 (23 septembre 1983);
- La Recommandation n° R (85) 20 relative à la protection desdonnées à caractère personnel utilisées à des fins de marketing direct (25 octobre 1985);
- La Recommandation n° R (86) 1 relative à la protection des données à caractère personnel utilisées à des fins de sécurité sociale (23 janvier 1986);
- La Recommandation n° R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police (17 septembre 1987);
- La Recommandation n° R (89) 2 sur la protection des données à caractère personnel utilisées à des fins d'emploi(18 janvier 1989).

4. Le Comité d'experts a, à présent, orienté son attention sur les divers problèmes soulevés par l'impact de la technologie de l'informatique sur les informations personnelles générées par la fourniture et l'utilisation de moyens de paiement. La société sans monnaie se développe par l'utilisation accrue de chèques pour régler des transactions. Ceci se poursuit actuellement par la prolifération de cartes plastiques. La technologie permet actuellement de parler en termes de monnaie électronique en permettant des transferts électroniques de

fonds aux points de vente grâce à l'utilisation de terminaux installés soit chez les détaillants soit à domicile. Les cartes de paiement sont en train de devenir "intelligentes" étant donné qu'on peut maintenant y intégrer des microprocesseurs.

5. Il incombait à un Groupe de travail du Comité d'experts sur la protection des données, spécialement constitué, d'étudier les conséquences de ces développements dans le domaine des moyens de paiement sur la collecte, l'enregistrement et le traitement des données à caractère personnel. Sous la présidence de M. J.-P. WALTER (Suisse), ce Groupe de travail s'est réuni à cinq reprises entre juin 1987 et janvier 1989 pour "examiner les problèmes de protection des données posés par certains aspects du secteur bancaire, en particulier, l'utilisation des cartes à mémoire, les transferts de fonds au point de vente, etc.".

6. Appuyé par le Comité plénier, le Groupe de travail a centré son attention sur le traitement automatique des données à caractère personnel qui sont collectées et enregistrées suite à la fourniture et à l'utilisation de moyens de paiement. Cette approche élargie lui a permis non seulement d'étudier les problèmes soulevés par les cartes à mémoire et les transferts électroniques de fonds (ainsi que stipulés spécialement dans le mandat), mais également d'autres moyens technologiques utilisés pour des règlements d'opérations (tels que les terminaux de banque à domicile, les distributeurs automatiques de billets). Etant donné que le point de départ reposait sur le traitement automatisé des données à caractère personnel dans le domaine des moyens de paiement, le Groupe de travail s'est intéressé aux moyens de paiement non issus de la technologie (par exemple chèques et cartes de paiement traditionnelles) car les données résultant de l'utilisation de moyens de paiement traditionnels sont susceptibles de faire l'objet d'un traitement automatisé à un stade ultérieur. Le Groupe de travail ne pouvait pas non plus passer sous silence la vaste gamme d'organismes qui offrent actuellement des moyens de paiement à leurs clients et qui ne sont pas des institutions bancaires au sens strict du terme. En outre, étant donné que les nouveaux moyens de paiement électroniques n'engendrent plus de relation discrète entre l'organisme fournisseur et l'utilisateur, l'on a estimé nécesaire d'inclure, dans le cadre de cette enquête, la gamme complète des acteurs intervenant dans le processus de paiement ou d'autres opérations connexes et qui pourraient être tenus de collecter et d'enregistrer des données à caractère personnel : les bénéficiaires de transactions, les exploitants des réseaux et tous les organismes fournissant des moyens de paiement.

7. Le Groupe de travail a noté un accroissement de la circulation des données à caractère personnel dans ce secteur dû à l'importance décroissante des transactions en espèces. Ceci est corroboré par le nombre important d'organismes, autres que les banques proprement dites, qui fournissent des moyens de paiement à un public qui ne demande qu'à bénéficier de leurs avantages par rapport aux espèces. Le Groupe de travail a noté, entre autres, que ces développements augmentaient la possibilité d'esquisser les habitudes des consommateurs puisque ces moyens de paiement laissent des traces du comportement économique chaque fois qu'ils sont utilisés. L'informatique permet de dresser une image cumulative (un profil) des transactions fragmentaires d'un consommateur.

8. La multiplicité des acteurs concernés, jointe au fait qu'un grand nombre d'organismes fournissant des moyens de paiement ne sont pas soumis aux principes du contrôle bancaire, soulèvent davantage de difficultés. Le caractère transnational des opérations de règlement par le biais des moyens de paiement ne peut pas non plus être ignoré.

9. Tout en notant que la Convention s'applique au traitement des données à caractère personnel dans tout ce domaine, le Groupe de travail a néanmoins jugé utile d'élaborer un

ensemble de pratiques d'information équitables destiné à minimiser les risques éventuels liés à la vie privée d'un individu par l'utilisation et la fourniture d'un moyen de paiement. En suivant l'approche utilisée pour des secteurs précédents, le Groupe de travail a, en consultation étroite avec le Comité plénier, adapté les principes contenus dans la Convention afin de réglementer les différentes étapes au cours desquelles la protection des données est considérée comme cruciale : la collecte, l'enregistrement, l'utilisation, la communication et la conservation de données à caractère personnel. Le Groupe de travail s'est aussi efforcé d'assurer les droits de la personne concernée dans ce secteur et a proposé une solution visant à minimiser les risques liés à la vie privée causés par le transfert vers d'autres pays de données à caractère personnel.

10. Les projets de principes résultant des discussions du Groupe de travail ont été examinés en détail lors de la 17e réunion du Comité d'experts sur la protection des données (7-10 mars 1989). Le Comité d'experts les a approuvés provisoirement, en fin de compte, tout en permettant à ses membres de proposer d'autres amendements avant la 18e réunion. Le Secrétariat a été chargé de rédiger un projet d'exposé des motifs pour examen et adoption à la 18e réunion.

11. Sur la base d'une série d'observations et de commentaires écrits émanant de diverses délégations et portant à la fois sur le projet de recommandation et sur le projet d'exposé des motifs, le Comité a entrepris un nouvel examen de ces deux textes à sa 18ème réunion (3-6 octobre 1989). Il a été estimé que les amendements effectués aux textes lors de la réunion devaient faire l'objet d'une mûre réflexion avant qu'une approbation finale ne puisse être donnée aux textes. A cette fin, les experts ont été invités à réexaminer les projets, avant la 19ème réunion du Comité plénier et à faire parvenir au Secrétariat leurs observations sur les nouveaux amendements.

12. A sa 19ème réunion (20-23 mars 1990), le Comité a approuvé les deux textes et décidé de les transmettre au Comité européen de Coopération Juridique pour examen et adoption. Le projet de recommandation ainsi que le projet d'exposé des motifs ont été approuvés par le CDCJ le 11 mai 1990, lors de sa 53ème réunion (8-11 mai 1990). La Recommandation n° R (90) 19 sur la protection des données à caractère personnel utilisées à des fins de paiement et autres opérations connexes a été adoptée par le Comité des Ministres du Conseil de l'Europe le 13 septembre 1990.

Commentaires détaillés

Préambule

13. A l'instar d'autres organismes des secteurs public et privé, les organismes qui fournissent des moyens de paiement ont largement bénéficié de la révolution technologique, notamment des techniques informatiques. S'agissant des "organismes fournissant des moyens de paiement", par exemple mais pas nécessairement les banques, l'informatique permet de gérer les comptes avec plus d'efficacité et de rapidité. Elle permet de rendre un meilleur service au client. Elle permet de traiter plus rapidement les opérations de règlement.

14. Dans le même temps, la télématique, qui a réuni les avantages de l'informatique et des télécommunications, a permis au particulier de profiter de toute une nouvelle gamme d'opérations financières. Avec le matériel nécessaire, ainsi qu'un lien de transmission de données, le particulier peut consulter de chez lui son compte en banque. Il peut commander

des chéquiers ou donner à sa banque des instructions pour effectuer un virement permanent en faveur de certains bénéficiaires. Les distributeurs automatiques de billets lui offrent des facilités analogues, y compris la possibilité de retirer des liquidités. Les terminaux sur le point de vente situés chez les détaillants, les commerçants et fournisseurs de service permettent au particulier de débiter électroniquement son compte et de donner à la banque l'ordre de créditer le compte du bénéficiaire de la transaction.

15. En plus du matériel, on trouve maintenant en circulation toutes sortes de cartes de paiement électroniques dont certaines sont indispensables pour permettre la réalisation des transactions mentionnées au paragraphe précédent. Certaines de ces cartes sont plus élaborées que d'autres. La carte à mémoire, ou carte à puce, peut réunir les qualités de la carte de crédit, de la carte de débit et de la carte de garantie des chèques tout en permettant de se servir du distributeur automatique de billets ou du terminal au point de vente.

16. Le Préambule reconnaît tous les avantages que l'informatique a apportés au domaine des moyens de paiement et aux autres opérations connexes. L'intérêt n'est pas exclusivement pour les banques et les autres organismes qui fournissent des moyens de paiement. Du point de vue du détaillant qui fait fonctionner un terminal au point de vente, le paiement qu'il perçoit est plus rapide. Le montant des liquidités qu'il est obligé de garder dans son magasin est moins important. Ses problèmes de tenue des comptes sont facilités. Du point de vue du particulier, les cartes de paiement électroniques lui donnent accès 24 heures sur 24 à des installations bancaires. Il n'est pas obligé de transporter des sommes importantes.

17. A l'aube de la société sans espèces, on estime opportun de réfléchir aux conséquences que l'informatique dans le secteur des moyens de paiement pourra avoir sur la vie privée des particuliers. Il ne faut pas voir la vie privée exclusivement dans l'optique des ingérences. Aux fins de la présente Recommandation, il faut plutôt y voir la capacité de l'individu à limiter et surveiller la collecte, l'enregistrement et l'utilisation par des tiers des données à caractère personnel qu'il communique dans le cadre d'une transaction. Le fait est que les transactions sans espèces et sans papiers donnent lieu à des enregistrements là où il n'en existait pas autrefois. Le paiement en espèces, et donc l'absence de documentation, donne au particulier l'avantage de pouvoir préserver son anonymat. Pratiquement, la valeur informative d'une transaction en espèces est nulle car l'individu laisse très peu de traces tant à l'égard de la nature de la transaction qu'à l'égard de son identité. Cela étant, les nouveaux moyens de paiement se caractérisent par l'enregistrement de données et l'intervention de différentes parties. Les moyens de paiement électroniques ont un potentiel qui leur permet de révéler une quantité considérable de données à caractère personnel du fait de leur utilisation. Une fois que des données sont saisies et enregistrées par des tiers, des techniques informatiques peuvent leur être appliquées afin de réunir les usages isolés et fragmentés des moyens de paiement pour en faire un profil permettant de surveiller le comportement économique du particulier et ses habitudes de consommation, et même ses mouvements. C'est ce type de risque qui fait l'objet des lignes directrices de la Recommandation.

18. Les banques au sens strict ne jouissent plus d'un monopole de la fourniture des moyens de paiement. Des organismes tels que les grands magasins et les compagnies pétrolières distribuent aussi leurs propres cartes de sociétés dont certaines peuvent être utilisées sur un terminal d'un point de vente situé dans les locaux de leurs filiales. Le Préambule constate que ces organismes ne sont pas liés par les principes du secret bancaire qui servent effectivement de complément utile aux principes de la protection des données lorsqu'il est

question de communication de données. Cela étant, il convient de rappeler que la protection des données est une notion plus large que celle du secret bancaire car elle fait référence à toutes les phases du traitement de données et non pas seulement à celle de la communication.

19. La Convention sur la Protection des Données, ainsi que la législation nationale en matière de protection des données, s'applique au traitement des données liées à la fourniture et à l'utilisation d'un moyen de paiement et à tous les acteurs qui jouent un rôle dans ce secteur. Néanmoins, ainsi que le déclare le Préambule, il a été jugé opportun de préciser les normes générales de la Convention pour mieux les adapter à la manière dont les informations à caractère personnel circulent dans le secteur des moyens de paiement ainsi qu'à la façon dont le traitement de données peut exercer une influence sur lui d'un point de vue tant qualitatif que quantitatif. C'est pourquoi la Recommandation présente des principes sur la manière dont les données à caractère personnel doivent être recueillies, enregistrées et utilisées, les conditions qui doivent régir leur communication, leur sécurité et leur conservation ainsi que les droits de la personne concernée à l'égard de ses données. Ces principes sont considérés comme une réponse éclairée et étudiée aux problèmes qui peuvent naître du traitement automatisé des données à caractère personnel en raison de la fourniture d'un moyen de paiement et de son utilisation.

20. Le texte ne se limite pas à "l'argent électronique". On remarquera d'après la partie consacrée au champ d'application et aux définitions que les opérations par chèques ou par cartes en plastiques sont régies par les principes. Après tout, en effet, la fourniture et l'utilisation de tels moyens de paiement donnent lieu à une collecte et à un enregistrement de données. Ces moyens de paiement ont une valeur informative lorsqu'on s'en sert. Ce qui est important, ce n'est pas le support utilisé pour le paiement, mais le fait que son utilisation entraîne un traitement automatisé de données à caractère personnel, au moment de l'utilisation ou lors d'une phase ultérieure.

21. Bien que le Préambule milite en faveur de la préservation de l'anonymat des parties à l'opération, autant que possible, malgré le recours croissant aux moyens électroniques de paiement, le texte ne prône pas le droit du particulier à régler ses transactions en espèces. Les auteurs de la Recommandation proposent tout simplement que l'individu devrait pouvoir choisir entre le règlement de ses transactions en espèces (et il peut avoir de bonnes raisons pour préserver son anonymat) et leur règlement par monnaie électronique avec les conséquences informatives que celle-ci entraîne.

22. En promouvant ces principes, les rédacteurs de la Recommandation ont aussi cherché à faciliter la libre circulation des données au-delà des frontières. Ainsi qu'on le verra au principe 10 de la Recommandation, les transactions financières ont un caractère plus transnational. Pour éviter les obstacles mis par le respect de la vie privée à l'échange transfrontière de données à caractère personnel liées à l'utilisation d'un moyen de paiement, on espère que le respect de ces principes dans tous les Etats membres du Conseil de l'Europe assurera un niveau équivalent de protection des données pour les données à caractère personnel auquelles s'applique la présente Recommandation. Ce principe va, bien entendu, de pair avec la nécessité de ratifier la Convention sur la protection des données.

Dispositif

23. Les principes et lignes directrices figurant dans la Recommandation sont destinés aux Gouvernements des Etats membres. Les Gouvernements sont invités à tenir compte de ces

principes et lignes directrices dans le cadre du domaine du droit tel que le droit bancaire, le droit du crédit à la consommation, etc. Les principes et lignes directrices peuvent bien entendu être repris dans le contexte du droit applicable à la protection des données. Il n'est pas nécessaire d'avoir recours à une législation contraignante pour tenir compte des principes et des lignes directrices. Leur respect pourrait être assuré à l'aide de codes de conduite ou d'autres mesures d'autodiscipline adoptés par les organismes fournissant des moyens de paiement. Il y a une tendance croissante à l'autoréglementation pour donner effet aux principes de la protection des données dans certains secteurs. Certaines grandes banques ont déjà adopté des codes de déontologie contenant des principes de bonne gestion des informations. On estime néanmoins que les codes de conduite et assimilés doivent être ratifiés par une instance supérieure, de préférence les organismes de contrôle établis en application de la législation relative à la protection des données. Gardant cela à l'esprit, les organismes fournissant des moyens de paiement ainsi que les bénéficiaires des opérations de réglement et les exploitants de réseaux de communication doivent négocier, peut-être par le biais de leurs associations représentatives si de telles associations existent, des mesures d'autoréglementation en concertation avec les autorités chargées de la protection des données.

24. Le texte invite aussi les Gouvernements des Etats membres à informer les autorités compétentes chargées de la protection des données lorsqu'elles existent, de l'existence de la Recommandation. On estime que ces autorités pourraient se servir du type de principes établis par la Recommandation pour régler les litiges relevant de la protection des données qui découlent de la fourniture et de l'utilisation d'un moyen de paiement. En portant la Recommandation à l'attention des autorités de surveillance et des principaux acteurs visés ci-dessus, on donne aussi aux différentes parties un ensemble tout prêt de principes sains pouvant constituer le fondement d'un code de conduite valable et efficace.

25. D'autres organisations internationales s'occupent aussi de problèmes liés à la fourniture et à l'utilisation de moyens de paiement - par exemple, la Commission de la Communauté européenne, l'OCDE et la CNUDCI. Les textes en cours de négociation au sein de ces organes ne se préoccupent pas essentiellement des problèmes de protection des données qui se posent en matière de moyens de paiement. On estime que les Gouvernements des Etats membres, dans leurs relations avec ces organismes internationaux, devraient d'une part, attirer l'attention de ces derniers sur la compétence particulière du Conseil de l'Europe dans le domaine de la protection des données et sur l'existence de la présente Recommandation et, d'autre part, les inviter à tenir compte des principes et lignes directrices qu'elle contient.

ANNEXE A LA RECOMMANDATION

1. Champ d'application et définitions

26. Ainsi que l'affirme le Préambule, le champ d'application des principes énoncés dans la présente Recommandation concerne avant tout le traitement automatisé des données à caractère personnel découlant de la fourniture et de l'utilisation d'un moyen de paiement. Certes, le traitement automatisé de données par des organismes fournissant des moyens de paiement se fondera sur différents sous-traitements manuels - par exemple, le particulier peut remplir un bref questionnaire précisant son nom, son âge, sa profession et son sexe. Néanmoins, étant donné que ces données seront ultérieurement mises sur ordinateur, il est normal que les principes énoncés dans la Recommandation, notamment celui de la

"collecte loyale et licite" qui se reflète dans le principe 3, s'appliquent aux phases de sous-traitements manuels.

27. Les références dans le paragraphe précédent aux sous-traitements manuels ne signifient pas que les données à caractère personnel qui font l'objet d'un traitement manuel sont incluses dans le champ d'application de la présente Recommandation. Cependant, les Etats membres sont bien entendu libres d'appliquer les principes énoncés dans la Recommandation aux données à caractère personnel enregistrées sur des supports manuels tels que les grands livres des banques et les répertoires. Une telle approche est conforme à l'article 3 paragraphe 2 c. de la Convention sur la Protection des Données et d'ailleurs, certains Etats membres appliquent effectivement leur législation en la matière aux données à caractère personnel qui font l'objet d'un traitement manuel. Il convient, évidemment, d'observer que le traitement manuel appartient de plus en plus au passé, compte tenu de la volonté de ce secteur et de la nécessité pour lui d'adopter de nouvelles technologies.

28. Il est utile de remarquer que les données manuelles sont protégées, dans une certaine mesure, par le principe du secret bancaire qui s'applique à la phase de communication quel que soit le mode de traitement. Il convient de garder cela à l'esprit dans le cadre du principe 5.

29. Le principe 1.1, alinéa 2 vise à énumérer les différents acteurs qui jouent un rôle dans ce domaine particulier. Par la suite, le texte prévoira de temps à autre des principes spécifiques concernant chacun d'entre-eux. On peut noter à ce stade que les organismes qui fournissent des moyens de paiement peuvent, en fait, être bénéficiaires de transactions. Par exemple, les compagnies pétrolières peuvent émettre des cartes privatives dont les particuliers peuvent se servir à des terminaux de vente situés dans les différentes stations services qui leur appartiennent. De même, il se peut que l'exploitant du réseau de communication, par exemple les P.T.T., puisse aussi profiter d'une opération de règlement effectuée par un particulier, l'exemple typique étant le réglement d'une facture de téléphone au moyen d'un terminal de banque à domicile.

30. Les données à caractère personnel que la présente Recommandation vise à protéger sont définies au principe 1.2. La définition proposée au principe 1.2 est maintenant bien établie et elle a été acceptée sans difficultés par les Gouvernements membres auxquels des recommandations sectorielles concernant la protection des données ont déjà été adressées.

31. La Recommandation ne fait pas expressément référence aux personnes morales. Les Etats membres ont, bien entendu, toute latitude pour appliquer les principes énoncés dans la Recommandation aux personnes morales qui, dans le cadre de cet instrument pourraient être les "bénéficiaires". En effet, après tout, les organismes fournissant des moyens de paiement enregistrent et traitent des données concernant les détaillants, les commerçants et les fournisseurs de services auxquels le particulier transfère des fonds dans le cadre d'une transaction. En outre, les organismes qui fournissent des moyens de paiement enregistrent et traitent des données concernant les entreprises qui gèrent l'utilisation d'un moyen de paiement pour leur compte. En conséquence, dans les pays où le régime de protection des données s'applique aussi aux personnes morales, les principes énoncés dans la présente Recommandation doivent aussi s'appliquer à ces dernières. Dans les pays où les personnes morales sont expressément exclues du champ d'application de la législation nationale relative à la protection des données, il faut être particulièrement attentif aux situations dans lesquelles les petits commerçants, les entreprises individuelles, etc., sont les destinataires d'une opération de transfert de fonds, que ce soit par chèque ou par support électronique, et

à l'égard de qui les données sont ensuite enregistrées par des organismes fournissant des moyens de paiement. Il peut n'être pas toujours facile de faire une distinction entre des données à caractère personnel concernant des individus et des données concernant des personnes morales lorsque la personne morale en question est en fait un individu.

32. Etant donné que les rédacteurs du texte ont cherché à viser essentiellement le traitement automatisé de données "lié à la fourniture et à l'utilisation d'un moyen de paiement ou d'autres opérations connexes" (voir principe 1.1 ci-dessus), il n'est pas étonnant que le texte donne une définition très large des moyens de paiement. On notera en particulier que la définition ne porte pas exclusivement sur la technologie. La définition ne se limite pas non plus aux moyens de paiement qui sont matériellement délivrés et ceci explique pourquoi le texte souligne la "fourniture" au lieu de "l'émission" ou de la "délivrance" d'un moyen de paiement. La définition proposée vise les différentes techniques informatiques, magnétiques, électroniques et télématiques, qui permettent d'échanger des fonds sans avoir besoin de papier - par exemple, les cartes à puce, les cartes à mémoire, les cartes à pistes magnétiques, les distributeurs automatiques de billets, et la banque à domicile, etc. Néanmoins, les rédacteurs ont aussi tenu à prendre en compte "l'argent non électronique". C'est pour cette raison que les chèques et les cartes non informatisées par exemple, figurent dans le champ d'application de la Recommandation. Contrairement à une opération de règlement en espèces, une transaction effectuée à l'aide d'un simple chèque ou d'une carte de crédit ou de débit non informatisée génère une valeur informative - par exemple, le nom et l'adresse du titulaire, ainsi que l'heure et le lieu de l'opération sont divulgués au bénéficiaire puis à la banque. Lorsque ces données font ensuite l'objet d'un traitement informatisé au sein de l'organisme fournisseur de tels moyens de paiement, ils doivent, selon les rédacteurs, relever carrément des principes énoncés dans la Recommandation.

33. Il y a, bien entendu, des limites aux types d'organismes auxquels s'applique l'expression "organismes fournissant des moyens de paiement". C'est seulement dans la mesure ou de tels organismes fournissent des moyens de paiement tels que ceux définis ci-dessus, que la définition leur est applicable. Les organismes en question peuvent être des institutions bancaires au sens strict (et donc être soumis aux principes du secret bancaire). Il peut aussi s'agir de grands magasins qui fournissent leurs propres cartes (privatives) de sociétés, sociétés de crédit immobilier, de compagnies pétrolières, de société de locations d'automobiles, etc. (non soumis aux principes du secret bancaire). Etant donné que la Recommandation ne s'applique qu'aux organismes fournissant des moyens de paiement dans la mesure où ils délivrent un moyen de paiement, l'intention des auteurs du texte n'était pas d'inclure ces organismes lorsqu'ils fournissent également des services d'investissement, lesquels peuvent être fournis en même temps qu'une transaction. Actuellement, il est par exemple possible de transférer électroniquement des actions en même temps que le paiement de la transaction. La Recommandation ne couvre pas le transfert de biens, mais seulement la partie du système concernant les moyens de paiement.

34. En outre, l'expression "organismes fournissant des moyens de paiement" a été définie soigneusement en vue de présenter une description claire et exacte de ce qui se passe en réalité dans ce secteur. Tout organisme peut, à la fois, fournir un moyen de paiement et gérer les implications financières liées à son utilisation. Alternativement, la gestion du compte peut être confiée à un autre organisme. Par exemple, un grand magasin peut émettre sa propre carte privative de société et charger une banque de s'occuper de la gestion au jour le jour du compte du client. En plus, tout organisme bancaire ou non-bancaire peut autoriser un tiers à fournir un moyen de paiement à un client, tout en

s'engageant à gérer le compte lui-même. Toutes ces différentes possibilités sont envisagées dans la définition d'"organismes fournissant des moyens de paiement". Les droits et devoirs des organismes qui reçoivent pour mandat (sous-contractants) de fournir ou de gérer des moyens de paiement pour le compte d'un autre organisme seront régis par le droit interne et déterminés par le contrat.

35. Les organismes évoqués au paragraphe précédent peuvent être privés ou publics. De même que la Convention sur la Protection des Données, la Recommandation s'applique à l'informatique dans les deux secteurs.

36. De façon à préserver la cohérence avec les activités connexes menées au sein d'autres instances internationales - principalement la Commission de la Communauté européenne, l'OCDE et la CNUDCI - les rédacteurs de la Recommandation ne se sont pas écartés de la définition reconnue de "l'exploitant du réseau de communication". L'exploitant du réseau de communication peut être de caractère public ou privé. Cette Recommandation ne couvre que l'exploitant du réseau de communication dans la mesure où il collecte, enregistre et traite des données à caractère personnel. S'il se contente de servir de lien de transmission sans collecter, enregistrer et traiter les données à caractère personnel, il n'est alors tenu de respecter que les principes relatifs à la sécurité des données (principe 8 de la Recommandation). Il est à noter qu'il existe déjà différents accords internationaux concernant la nécessité, pour les exploitants de réseaux de communication, de s'assurer de la sécurité de leurs systèmes de transmission. La ligne de communication peut aussi être louée à un réseau général de télécommunications - par exemple comme dans le cas du système SWIFT ou dans celui des réseaux interbanques. La présente Recommandation concerne l'exploitant du réseau de communication uniquement dans la mesure où il est responsable de l'exploitation d'un système. Les principes ne s'appliquent pas aux autorités chargées des télécommunications qui se contentent de fournir des services de logiciels, mais ils s'appliquent aux exploitants de ces services.

2. Respect de la vie privée

37. Les rédacteurs des recommandations sectorielles relatives à la protection des données ont l'habitude de commencer les principes de protection des données par une déclaration générale concernant la nécessité de respecter la vie privée de l'individu. Il s'agit là d'un usage considéré comme très important car il permet d'indiquer clairement d'une part, qu'il y a des liens entre la protection des données et la vie privée de l'individu et, d'autre part, que les droits de l'homme sont en jeu lorsque des informations à caractère personnel circulent au sein de la société dans son ensemble ou dans certains de ses secteurs. C'est dans cette perspective que le principe 2 contient une liste exhaustive des différentes phases du traitement où il peut être porté atteinte à la protection de la vie privée/des données. Le texte attire aussi l'attention des principaux acteurs qui jouent un rôle dans ce secteur sur la nécessité d'assurer le respect du caractère confidentiel des données à caractère personnel. Les "mesures nécessaires" évoquées dans le texte seront étudiées plus en détail dans le cadre des principes relatifs à l'utilisation et à la sécurité des données.

3. Collecte et enregistrement des données

38. Les alinéas a. et c. de l'article 5 de la Convention sur la Protection des Données énoncent respectivement le principe de la collecte loyale et licite des données et celui de la limitation de l'enregistrement. Comment ces principes peuvent-ils acquérir une signification concrète dans le cadre de la collecte et de l'enregistrement des données à

caractère personnel utilisées à des fins de paiement et d'autres opérations connexes et englober les différents acteurs qui y jouent un rôle? Le principe 3 de la Recommandation cherche à établir un ensemble de lignes directrices concernant la manière dont les données doivent être recueillies et enregistrées, à l'intention des organismes fournissant des moyens de paiement, des exploitants de réseaux de communication et des bénéficiaires.

39. Le principe 3.1 traite de l'enregistrement des données à caractère personnel par des organismes fournissant des moyens de paiement. En quelques mots, les données enregistrées doivent être "nécessaires à la mise à disposition du moyen de paiement et des services liés à son utilisation y compris à des fins de contrôle". En d'autres termes, pour reprendre la terminologie de l'article 5 alinéa c. de la Convention sur la Protection des Données, les données à caractère personnel enregistrées doivent être adéquates, pertinentes et non excessives par rapport à ces finalités. S'agissant de la décision de fournir un moyen de paiement à un individu, l'organisme fournisseur peut exiger des informations concernant, par exemple, le nom, l'âge, l'adresse, le sexe, la profession et les revenus du demandeur et toutes autres informations qui sont nécessaires pour évaluer correctement les risques accompagnant la mise à disposition de moyens de paiement. Les organismes fournissant des moyens de paiement doivent éviter les longs questionnaires réclamant des informations sans aucun rapport avec la fourniture d'un moyen de paiement. Comme cela ressort du principe 3.3, il se peut que l'organisme fournissant un moyen de paiement ait besoin d'évaluer les risques qu'il court en raison de la fourniture d'un moyen de paiement à un demandeur - par exemple, va-t-il laisser accumuler des dettes importantes, va-t-il exploiter abusivement le moyen de paiement en dépassant intentionnellement ses limites de crédit ? Ces évaluations peuvent exiger que des tiers soient consultés. Le principe 3.1 admet que les données ainsi collectées puissent être enregistrées ("à des fins de contrôle").

40. Les types d'informations personnelles visées à ce stade peuvent être qualifiées de données a priori. Il arrive aussi qu'il faille réunir des données a posteriori pour gérer le compte du titulaire du moyen de paiement lorsqu'il s'en sert à des fins de transaction. C'est l'enregistrement de ces données a posteriori qui peut être à l'origine de problèmes relevant de la protection des données. En effet, les différents usages d'un moyen de paiement par une personne peuvent révéler certains aspects de ses préférences de consommateur, de l'endroit où elle se trouve, de ses déplacements, voire de sa vie intime. Le principe 3.1 souligne à ce stade que seules devraient être collectées et enregistrées les données nécessaires pour permettre les services liés à l'utilisation du moyen de paiement. On verra que les alinéas suivants du principe 3 visent à imposer des limites supplémentaires à l'enregistrement de données personnelles lorsque l'individu utilise le moyen de paiement.

41. Le texte admet que les organismes fournissant des moyens de paiement puissent confier la collecte, l'enregistrement et le traitement de données à caractère personnel à un mandataire. Il s'agit là d'une caractéristique normale du secteur des moyens de paiement. Conformément au principe 3.2, le mandataire ou "sous-traitant" doit être tenu par contrat de veiller à ce que les données ne soient pas exploitées à d'autres fins que celles précisées par l'organisme fournissant le moyen de paiement.

42. Le principe 3.3 donne des indications complémentaires expliquant comment les organismes fournissant des moyens de paiement peuvent collecter les données de manière loyale et licite. On considère que l'individu doit être la principale source d'information. On admet que d'autres sources peuvent être consultées afin de déterminer s'il s'agit ou non d'une personne qui convient pour recevoir un moyen de paiement. Les sources en question peuvent résider dans des informations accessibles à tous - par exemple, les annuaires

téléphoniques et les listes électorales. La consultation de fichiers publics peut aider à savoir si la personne est bien celle qu'elle prétend être, si son adresse est exacte, si elle a sa résidence habituelle dans le pays, etc. Les organismes fournissant des moyens de paiement peuvent aussi vouloir vérifier la solvabilité du demandeur d'un moyen de paiement. A cette fin, ils peuvent avoir besoin de consulter des agences de renseignements sur le crédit ou des fichiers contenant des listes de personnes qui ont été déclarées en faillite. Cela étant, le principe 3.3 insiste sur la nécessité de ne pas exclure l'individu du circuit d'information. A l'exception éventuelle de fichiers accessibles au public en général, l'individu doit être pleinement avisé de la possibilité que des tiers peuvent être consultés, des types de sources qui peuvent être consultées et des conditions dans lesquelles ces consultations peuvent avoir lieu. Il doit être libre de refuser son consentement pour la consultation de certaines sources. Il peut, bien entendu, courir certains risques s'il refuse effectivement de permettre à l'organisme auquel il s'est adressé pour obtenir un moyen de paiement de consulter certaines sources - le moyen de paiement désiré peut ne pas lui être fourni. L'individu doit être clairement informé du type de risques auxquels il s'expose s'il refuse de consentir à la consultation de certaines sources.

43. Il se peut que l'organisme fournissant le moyen de paiement ait besoin de consulter des tiers lorsque l'individu se sert d'un moyen de paiement. Par exemple, si celui-ci a un découvert qui ne cesse d'augmenter, il peut être nécessaire de consulter une agence de renseignements sur les mauvais payeurs afin de déterminer si la personne en question doit de l'argent à d'autres organismes financiers. Là encore, l'intéressé doit être clairement informé du fait que l'organisme fournissant le moyen de paiement peut, dans certaines circonstances précises, après la fourniture du moyen de paiement, exercer un contrôle à son égard en ayant recours à des tiers.

44. Alors que les principes 3.1 et 3.3 s'adressent aux divers organismes fournissant des moyens de paiement, le principe 3.4 concerne le bénéficiaire d'une opération de règlement. Il impose une stricte condition de limitation de l'enregistrement. Les détaillants, les commerçants et les fournisseurs de services doivent parfois demander à l'individu de faire la preuve de son identité afin de certifier qu'il s'agit de la personne habilitée à utiliser le moyen de paiement. En outre, les bénéficiaires peuvent éprouver la nécessité de prendre contact avec la banque ou autre organisme fournisseur du particulier afin de déterminer sa solvabilité. Des détaillants disposent souvent de listes de cartes de paiement ou de chéquiers volés ou perdus qui sont distribuées par les organismes fournisseurs. De telles listes peuvent aussi préciser les restrictions de crédit imposées par l'organisme fournisseur au titulaire. Les détaillants peuvent consulter ces listes vu qu'elles sont liées au processus de la détermination de la validité de paiement. La collecte et l'enregistrement des données afférentes à ces contrôles sont admis. La durée pendant laquelle ces données peuvent être conservées fera l'objet du principe 11. Le bénéficiaire n'a cependant nul besoin de garder la trace de la nature exacte de l'opération effectuée par l'individu sous forme nominative. Dans le cadre, par exemple, d'une action en justice en cas d'achat de marchandise défectueuse, ou afin d'assurer un service après-vente, un simple reçu anonyme précisant la date et l'achat est suffisant.

45. Comme il ressort de la discussion sur "les organismes fournissant des moyens de paiement", un tel organisme, au lieu de fournir un moyen de paiement, peut se limiter à la gestion du compte d'un client à qui un moyen de paiement a été fourni par un autre organisme. Le premier organisme peut, par exemple, permettre audit client de dépasser son crédit ou lui accorder un prêt ou d'autres services financiers liés à l'utilisation du moyen de paiement. La fourniture de tous ces différents services sera remboursée par l'organisme

fournissant le moyen de paiement. A bien des égards, donc, l'organisme en question devrait être considéré comme bénéficiaire et être assujetti en conséquence aux exigences du principe 3.4.

46. Lorsque des transactions sont effectuées par l'individu à l'aide d'un moyen de paiement - par exemple, transfert électronique de fonds au moyen d'un terminal au point de vente, utilisation d'une carte de paiement électronique dans un distributeur automatique ou achat de biens et de services à l'aide d'une carte de crédit - certains détails concernant la transaction doivent inévitablement être communiqués à l'organisme fournissant le moyen de paiement, afin que le compte du titulaire puisse être débité et celui du bénéficiaire crédité ou bien pour transférer les avoirs du titulaire d'un compte à un autre, conformément aux instructions données au guichet automatique ou à un terminal de télépaiement. Le principe 3.5 impose une limitation à l'enregistrement de telles données. Celles-ci ne doivent être enregistrées que dans la mesure nécessaire pour valider et prouver la transaction du particulier ainsi que pour réaliser les services liés à l'utilisation d'un moyen de paiement, l'exemple typique étant le transfert de fonds du compte de l'individu à celui du bénéficiaire. L'organisme fournisseur n'a nul besoin de conserver des dossiers détaillant la nature de la transaction effectuée par le particulier à l'aide d'un moyen de paiement, mais il est inévitable que la nécessaire divulgation du nom et du numéro de compte du bénéficiaire indique le type de transaction qui a été effectuée. Il est évident que ce principe ne porte atteinte ni au droit du titulaire du moyen de paiement de mentionner, s'il le souhaite, l'objet de la transaction effectuée, ni au besoin de l'organisme fournissant le moyen de paiement d'effectuer l'objet demandé par le titulaire. Le principe 3.5 reconnaît aussi que le droit interne peut exiger que des données à caractère personnel soient collectées et enregistrées par des organismes fournissant des moyens de paiement. A titre d'exemple, le droit interne peut demander aux banques de garder la trace de tous les transferts de fonds à destination de l'étranger au-delà d'un certain montant.

47. Bien que le principe 3.5 ne le précise pas, on estime que les organismes fournissant des moyens de paiement peuvent faire usage de techniques du credit scoring pour évaluer les différents risques liés à l'octroi du crédit. Les modèles statistiques qui servent à évaluer de tels risques sont basés sur des ensembles de données anonymes. Néanmoins, les organismes fournissant des moyens de paiement peuvent avoir besoin d'enregistrer des données nominatives pendant une période courte afin qu'elles puissent être comparées aux modèles de risques et à des fins de prévisions statistiques dans un cas particulier. On estime qu'une période limitée et transitoire d'enregistrement de données à caractère personnel est aussi admise.

48. Les principes 3.1 à 3.5 concernent la nécessité d'éviter que trop de données à caractère personnel ne soient collectées et enregistrées par les organismes fournissant des moyens de paiement et les bénéficiaires d'opérations de règlement. Il est maintenant reconnu que l'informatique maximalise la quantité de données à caractère personnel qui peuvent être collectées, enregistrées et traitées. Pour répondre à cette préoccupation, la politique de protection des données établit des principes tels que ceux du caractère adéquat, pertinent et non excessif. Cela étant, l'informatique elle-même peut aussi apporter des solutions techniques permettant de minimiser la quantité de données à caractère personnel qui peuvent être légitimement collectées et enregistrées. C'est dans cette optique que le principe 3.6 préconise l'intégration de dispositifs dans, par exemple, les cartes de paiement électroniques ou le matériel comme les terminaux aux points de vente ou les terminaux de télépaiement, afin de veiller à ce que des données qui sont sans intérêt, inutiles ou

excessives ne soient pas communiquées à l'organisme fournissant le moyen de paiement ni conservées par le bénéficiaire.

49. Les limitations d'enregistrement ne s'appliquent pas uniquement aux organismes fournissant des moyens de paiement et aux bénéficiaires. L'exploitant du réseau de communication, dans la mesure où il collecte, enregistre et traite les données à caractère personnel, plutôt que de se contenter de servir de lien de transmission, comme défini au principe 1.2, doit également être limité quant à la quantité de données à caractère personnel qui peuvent être enregistrées. C'est pourquoi le principe 3.7 est consacré au besoin de délimiter la quantité de données à caractère personnel qu'il peut collecter et enregistrer, en tenant compte de ses fonctions dans le secteur des moyens de paiement.

50. Le principe 3.8, deuxième alinéa, est tout à fait clair sur la question des données sensibles des types visés à l'article 6 de la Convention sur la Protection des Données, à savoir les données révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, ainsi que les données à caractère personnel relatives à la santé ou à la vie sexuelle. Ces données ne peuvent être ni collectées ni enregistrées. Rien ne justifie la collecte et l'enregistrement de ce type de données sensibles pour la fourniture d'un moyen de paiement. Il est néanmoins admis que les organismes fournissant des moyens de paiement soient fort désireux de connaître les antécédents délictueux du demandeur d'un moyen de paiement. Il est manifestement contraire aux intérêts de l'organisme en question de fournir un moyen de paiement à un fraudeur. Le premier alinéa du principe 3.8 envisage seulement que les organismes fournissant des moyens de paiement traitent des données relatives aux condamnations pénales d'un individu uniquement lorsqu'elles sont manifestement pertinentes pour la détermination du point de savoir si l'individu est une personne à laquelle il convient ou non d'accorder un moyen de paiement. Les infractions récentes en matière de fraude et d'escroquerie sont, de toute évidence, pertinentes. Leur traitement est donc justifié, à moins qu'il ne soit possible d'obtenir par ailleurs les informations nécessaires pour déterminer si l'individu pourrait se voir octroyer un moyen de paiement. Cela étant, le traitement des infractions au code de la route commises par le demandeur est manifestement injustifié. Ces infractions n'ont aucun rapport avec la possibilité pour lui de se voir délivrer ou de continuer à employer un moyen de paiement.

51. Néanmoins, même lorsque le traitement de condamnations pénales est manifestement justifié, le traitement des données doit satisfaire aux conditions énoncées au principe 3.8, alinéa 1, c'est-à-dire que l'individu doit donner son consentement exprès et éclairé à leur traitement ou que celui-ci ne doit être réalisé que dans le respect de toute garantie prévue par le droit interne.

4. Utilisation des données

52. La nature fournie des informations à caractère personnel enregistrées par les organismes fournissant des moyens de paiement ainsi que par les bénéficiaires, associée à la multiplicité des acteurs qui interviennent dans le secteur des moyens de paiement, a conduit les spécialistes de la protection des données à réfléchir sur la nécessité de définir avec clarté les finalités légitimes pour lesquelles les informations peuvent être utilisées. On estime que les finalités précisées au principe 4.1 reflètent bien l'article 5.b de la Convention sur la Protection des Données dans la mesure où les organismes fournissant des moyens de paiement collectent et enregistrent des données à caractère personnel. Par exemple, il va de soi que les données à caractère personnel enregistrées par l'organisme fournissant des moyens de paiement peuvent être utilisées pour gérer le compte de la personne concernée -

exécuter ses instructions s'agissant de débiter ou de créditer son compte, lui fournir un relevé pour lui permettre de contrôler ses dépenses, etc. Les organismes fournissant des moyens de paiement peuvent aussi être tenus d'adopter des mesures pour éviter que le moyen de paiement ne fasse l'objet d'abus s'il tombe entre de mauvaises mains, ou si le titulaire a l'habitude d'être à découvert parce qu'il dépasse la ligne de crédit qui lui a été accordée. C'est dans cette optique que le principe 4.1 reconnaît que les organismes fournissant des moyens de paiement peuvent utiliser les données dans ces circonstances afin de réduire les abus dans toute la mesure du possible - par exemple, en diffusant le nom et le numéro de compte du titulaire auprès des banques ou en diffusant ces informations aux commerçants et détaillants sous la forme d'une liste d'opposition.

53. On notera que le principe 4.3 autorise l'interconnexion de différents fichiers de données à caractère personnel pour permettre la réalisation des finalités évoquées au principe 4.1.

54. L'un des principaux risques que font peser sur la vie privée la fourniture et l'utilisation d'un moyen de paiement réside dans le fait que, lorsque des méthodes de traitement automatisé des données sont appliquées aux données à caractère personnel créées grâce à l'utilisation d'un moyen de paiement, il est possible de construire électroniquement des profils relatifs au comportement individuel, notamment en ce qui concerne les habitudes de dépenses et les préférences des consommateurs. Ces profils ont une valeur commerciale. Ils peuvent servir au ciblage de fractions de la population par des entreprises de marketing direct, permettant ainsi à ces dernières d'établir des relations commerciales avec le particulier en envoyant à celui-ci des informations reflétant ses goûts en matière de littérature, de vacances, de produits d'usage courant, etc.

55. Les rédacteurs de la présente Recommandation ont cherché à imposer des limites à la commercialisation ou à l'utilisation secondaire de données a posteriori ainsi qu'on l'a vu à un stade antérieur. C'est dans cette optique que les principes 4.2, 4.3 et 4.4 énoncent des lignes directrices pour la protection des données à caractère personnel qui peuvent être utilisées à des fins de marketing direct ou de promotion. Il va sans dire que ces lignes directrices sont calquées sur les principes établis par la précédente recommandation du Comité des Ministres en la matière, à savoir la Recommandation n° R (85) 20.

56. Le principe 4.2 permet aux organismes fournissant des moyens de paiement de se servir des données qu'ils ont enregistrées pour commercialiser et promouvoir les différentes gammes de services, financiers ou autres, qu'ils proposent. L'individu doit être informé, et le principe 4.2 souligne que cette information doit lui être communiquée par écrit, du fait qu'après qu'un moyen de paiement lui a été fourni, il peut recevoir une brochure l'invitant à demander, par exemple, des plans d'épargne, des services d'investissement, ou d'autres services à caractère non financier (par exemple voyage) proposés par l'organisme. La communication écrite doit mentionner le fait que l'individu n'est pas obligé d'avoir son nom sur la mailing-list de l'organisme fournisseur. Pour déterminer s'il convient d'accorder à un individu un service particulier (financier ou autre), l'organisme fournisseur peut avoir besoin de contrôler le comportement financier de l'individu. Le principe 4.3 autorise l'interconnexion de fichiers à de telles fins à condition que l'individu ait manifesté expressément son intérêt à recevoir des informations sur les différents services offerts par l'organisme fournisseur conformément aux dispositions du principe 4.2. Il serait injuste de refuser un moyen de paiement à un individu qui informe un organisme fournissant un moyen de paiement qu'il ne souhaite pas recevoir de brochure commerciale ou promotionnelle. Cela constituerait un abus de position dominante et réduirait à néant la nécessité d'informer par écrit l'individu de son droit de ne pas figurer

sur une mailing-list (principe 4.2, 1er alinéa). Dans certains systèmes juridiques européens, une telle situation peut donner lieu à ce que l'on appelle un "abus de droit". C'est pour cette raison que le principe 4.2, alinéa 2, prévoit que l'individu soit informé du fait que son refus de ne pas figurer sur une mailing-list ne nuira en rien à la décision de lui accorder un moyen de paiement ou de lui permettre de continuer à l'utiliser s'il retire par la suite son consentement.

57. Lorsque des interconnexions de fichiers ou des techniques de croisement, effectuées en vue de tirer des conclusions relatives à l'individu, ne sont pas compatibles avec les finalités indiquées au principe 4.3, l'organisme fournissant des moyens de paiement doit, sauf si le droit interne l'autorise, obtenir le consentement exprès et éclairé de l'individu avant toute interconnexion des divers fichiers contenant des données personnelles le concernant (principe 4.3, second alinéa).

58. Il est exact que l'utilisation d'un moyen de paiement révèle parfois certaines données sensibles, telles que celles mentionnées à l'article 6 de la Convention sur la Protection des Données. Par exemple, les organismes fournissant des moyens de paiement peuvent avoir la possibilité de déterminer les opinions politiques ou religieuses de l'individu lorsque celui charge la banque de débiter son compte pour créditer celui d'une association politique ou d'une institution religieuse. Les ordres de virement permanents en faveur de certains clubs ou associations peuvent aussi révéler des aspects de sa vie sexuelle. Le principe 4.4 est tout à fait clair quant à l'usage qui peut être fait de telles données transactionnelles. Celles-ci ne peuvent être utilisées à aucune fin et certainement pas à des fins de marketing ou de promotion même s'il s'agit de fournir des services financiers.

59. La technologie est maintenant parvenue à un stade, où, entre autres, les cartes électroniques peuvent être de nature multifonctionelle. Une carte à mémoire, par exemple, peut être en même temps un moyen de paiement et un dossier médical portable contenant les antécédents médicaux du titulaire, le traitement qu'il suit, etc. Une telle carte peut aussi servir de moyen d'accès à des locaux protégés. Il y a des risques s'il est possible d'accéder aux données financières figurant dans la mémoire de la carte lorsque celle-ci est utilisée dans le cadre d'une de ses autres nombreuses fonctions. C'est pourquoi il est recommandé que la carte soit conçue de manière à éviter l'accès aux données financières enregistrées dans la mémoire lorsque le titulaire se sert de la carte à d'autres fins.

5. Communication de données

60. Le commentaire fait fréquemment référence à la notion de secret bancaire qui trouve son expression dans les ordres juridiques des Etats membres en tant que principe de droit coutumier ou en tant que disposition du code pénal ou du code civil, voire en tant que norme constitutionnelle. Ainsi qu'on l'a dit plus haut, le secret bancaire concerne la communication à des tiers de données à caractère personnel en dehors du cadre de l'institution bancaire (au sens strict du terme). Même si les différentes situations dans lesquelles les Etats membres permettent de lever le voile du secret bancaire se reflètent plus ou moins dans les dispositions du principe 5, il est à noter que le principe 5 est un principe indépendant et distinct du principe du secret bancaire et concerne plutôt les hypothèses qui autorisent l'utilisation (communication de données à caractère personnel à des fins autres que celles pour lesquelles elles ont été collectées et enregistrées). Il convient de remarquer que le principe de la communication vise non seulement le transfert de données à des tiers qui assument des fonctions sans aucun rapport avec la fourniture de services financiers, mais aussi aux filiales d'organismes fournissant des moyens de

paiement qui se lancent dans des activités sans aucun rapport avec la fourniture de moyens de paiement. En d'autres termes, la communication de données à caractère personnel par un organisme fournissant un moyen de paiement, au sein du même groupe, est aussi régie par les dispositions du principe 5 lorsque le groupe se compose d'agences de voyage, de compagnies d'assurance, etc.

61. Bien que le texte ne le dise pas expressément, les Etats membres pourraient utilement réfléchir à l'opportunité d'élargir le principe du secret bancaire à tous les organismes qui fournissent des moyens de paiement, au lieu de le limiter aux banques au sens strict.

62. Les types de situations évoquées du principe 5.1 (a) au principe 5.1 (d) appellent les remarques suivantes :

- les "obligations prévues par le droit interne" ne se limitent pas aux obligations légales de communiquer des données financières, par exemple au fisc ou à la police. Une décision de justice peut obliger un organisme fournissant des moyens de paiement à divulguer des données, par exemple dans le cadre d'une action en divorce ou en séparation impliquant la personne concernée et son conjoint. Une obligation peut aussi apparaître lorsque l'intérêt général exige, dans un but de prévention de la criminalité, la divulgation de données à caractère personnel. Il est possible qu'un organisme fournissant des moyens de paiement soupçonne fortement le titulaire d'un compte de blanchir par son intermédiaire des fonds acquis illégalement. De telles circonstances justifieraient la communication des données pertinentes à la police ;

- un organisme fournissant des moyens de paiement peut avoir besoin de protéger ses intérêts légitimes en communiquant des données relatives à un client qui s'est vu fournir un moyen de paiement lorsqu'il cherche à recouvrer, dans le cadre d'une action en justice, une créance due aux dépenses excessives du client. Pour que le litige soit résolu en faveur de l'institution demanderesse, il peut être nécessaire de saisir la justice des transactions effectuées par le client. Il peut arriver aussi que l'organisme fournissant le moyen de paiement ait besoin de diffuser un numéro de carte de crédit ou le nom du titulaire d'un chèque afin d'avertir les détaillants, commerçants, etc., qu'ils ne doivent pas accepter la carte de crédit ou le chèque car elle/il figure sur une "liste d'opposition". Il est à noter que les intérêts de l'organisme fournissant le moyen depaiement qui sont en jeu devraient primer clairement sur les intérêts de l'individu à la non-communication des données le concernant ;

- le consentement de l'individu à la communication à des tiers des données le concernant par l'organisme fournissant le moyen de paiement doit être "exprès et informé". Le consentement implicite ne satisfait pas à cette condition. En conséquence, s'il arrive que des organismes fournissant des moyens de paiement communiquent régulièrement aux organismes de renseignements sur le crédit des informations relatives au titulaire de chèques sans provision, l'individu devrait, aumoment de conclure le contrat avec un organisme pour la fourniture d'un moyen de paiement, être clairement averti de cette possibilité et y consentir expressément ;

- certains ordres juridiques permettent la constitution d'organismes informateurs ou enregistreurs qui reçoivent de la part des organismes fournissant des moyens de paiement des informations concernant le fait que le titulaire d'un moyen de paiement excède sa ligne de crédit et donc ne respecte pas les conditions régissant l'utilisation du moyen de paiement. Le texte admet qu'il puisse y avoir un tel système pour

accroître la sécurité de paiement dans le secteur des moyens de paiement. A certains égards, les dispositions du principe 5.1 (d) sont étroitement liées à celles du principe 5.1 (b). Il va sans dire que les activités informatiques du type d'organes visés à l'alinéa (d) sont soumises aux conditions fixées par lalégislation interne relative à la protection des données et, plus particulièrement, à la surveillance exercée par les organes de contrôle établis conformément à cette législation.

63. Ainsi qu'on l'a vu plus haut dans le commentaire, les organismes fournissant des moyens de paiement peuvent sous-traiter à des tiers différents aspects de leurs activités. Par exemple, il se peut qu'une société émettrice d'une carte privative engage les services d'une banque pour gérer le compte du particulier auquel la carte est délivrée. Il se peut aussi qu'un organisme fournissant un moyen de paiement loue les activités informatiques qui accompagnent la fourniture et l'utilisation de celui-ci. Ou bien l'exploitant du réseau de communication peut aussi avoir besoin des données à caractère personnel enregistrées par la banque pour permettre d'établir le lien entre l'organisme fournissant le moyen de paiement, le bénéficiaire et la personne concernée. Le principe 5.2 de la Recommandation reconnaît que cette sorte de communication est de l'ordre normal des choses.

6. Publicité

64. La législation interne en matière de protection des données oblige généralement les utilisateurs de données à déclarer ou enregistrer ou notifier d'une autre façon leurs activités informatiques auprès des autorités de surveillance compétentes. Dans certains cas, l'autorisation peut être exigée avant que le traitement des données ne puisse avoir lieu. Le principe 6 rend compte de cette situation. Les éléments qui y sont évoqués doivent normalement être portés à l'attention des organes de contrôle qui, à leur tour, adoptent des mesures pour rendre publiques les informations qui leur ont été communiquées. C'est ainsi que l'individu est informé de "l'existence d'un fichier automatisé de données à caractère personnel, ses finalités principales, ainsi que l'identité et la résidence habituelle ou le principal établissement du maître du fichier" (article 8.a de la Convention sur la protection des données). L'opportunité de rendre plus transparentes les activités informatiques des organismes fournissant des moyens de paiement, des bénéficiaires et des exploitants des réseaux de communication, dans la mesure où ils collectent, enregistrent et traitent des données à caractère personnel, peut aussi être renforcée par eux-mêmes. Il existe des moyens pratiques pour y parvenir. Par exemple, la documentation produite par les organismes fournissant des moyens de paiement peut servir de véhicule pour informer l'individu du genre d'éléments figurant dans le principe 6.

7. Droit d'accès et de rectification

65. Si le principe 6 est considéré comme le reflet de l'article 8.a de la Convention, le principe 7 est l'expression concrète de l'article 8.b et c.

66. On remarquera qu'aucune exception n'est formulée à l'égard du type de données à caractère personnel auxquelles peut accéder la personne concernée. Il est néanmoins possible que certains Etats membres restreignent l'accès à des données factuelles, à l'exclusion des appréciations, opinions ou évaluations subjectives relatives à des questions telles que le risque que présente un individu du point du vue du crédit. Cela étant, il n'y a en principe aucune raison pour que le droit d'accès ne s'étende pas aussi à de telles données.

67. Le principe 7.1 souligne la nécessité de remettre les données demandées en vertu de l'exercice du droit d'accès sous une forme compréhensible par l'individu. C'est pourquoi les données ne doivent pas être codées. Il s'agit, après tout, de données qui le concernent et il doit être en mesure d'apprécier leur importance. Le principe 7.1 envisage aussi d'autoriser l'individu à accéder aux données à caractère personnel figurant sur le moyen de paiement lui-même - notamment sur les cartes à piste magnétique ou les cartes à microcircuit/puce/mémoire. A cet effet, l'individu doit obtenir si possible, l'accès à un lecteur adéquat éventuellement sous le contrôle de l'organisme fournissant ce moyen de paiement, afin de lui permettre de voir ce qui échappe à l'œil nu. S'il n'y a pas de lecteur disponible, l'individu devrait pouvoir recevoir les informations sous une forme intelligible, par exemple, sur un imprimé reproduisant les informations portées sur sa carte et auxquelles il a le droit d'accéder en vertu de la législation nationale. Encore une fois, il s'agit des données le concernant et il doit avoir le droit d'y accéder.

68. L'importance du droit d'accès est indiqué au principe 7.2. Il s'agit du droit donné à l'individu de s'assurer que l'organisme fournissant le moyen de paiement respecte les principes établis par la Recommandation.

69. Il existe des moyens pratiques pour adopter les "mesures adéquates" visées au principe 7.3 en vue de sensibiliser la personne concernée au fait qu'elle jouit des droits énoncés aux principes 7.1 et 7.2. Les brochures et documents promotionnels produits par l'institution financière ou les relevés que celle-ci fournit régulièrement au client constituent des moyens utiles d'information de l'individu sur ses droits d'accès, de rectification et d'effacement et sur la manière dont il peut les exercer.

70. Le Comité intergouvernemental d'experts sur la protection des données, qui était chargé d'élaborer la Convention sur la Protection des Données ainsi que les recommandations sectorielles antérieures, a tenu à s'assurer que les larges principes énoncés dans la Convention conservent leur sens et leur efficacité face à l'évolution technologique. Le Comité a constaté, entre autres, que le traitement de données au sein des organisations ne se caractérisait plus par un enregistrement et des méthodes de traitement centralisés. Il y a maintenant une tendance à la gestion de réseaux et aux systèmes d'informatique répartis. Ces méthodes informatiques décentralisées ont des répercussions sur les droits de la personne concernée. Par exemple, il n'est parfois plus possible à l'individu d'avoir accès à un fichier unique contenant la totalité des informations détenues à son sujet par certains organismes. Il peut y avoir, à la place, une multitude de fichiers différents. Le Comité a traité cette question dans son rapport intitulé "Technologies nouvelles - un défi à la protection de la vie privée?" adopté par le Comité des Ministres en 1988. Le rapport préconise l'existence d'un fichier "logique" au sein des organismes qui exploitent des systèmes d'informatique répartis. Un tel fichier logique permettrait de finir par localiser, grâce à des méthodes de recherche, les données à caractère personnel dispersées dans le réseau. Les rédacteurs de la Recommandation ont repris cette idée au principe 7.4 pour veiller à ce que l'individu puisse, pour reprendre la terminologie de la Convention sur la Protection des Données, sans délai ni frais d'accès excessifs, avoir accès à la totalité des informations détenues à son sujet par un organisme fournissant un moyen de paiement.

8. Sécurité des données

71. La sécurité des données est une question clef de toute politique de protection des données. Il devient de plus en plus important de réfléchir aux moyens permettant d'assurer l'intégrité et la confidentialité des données à caractère personnel en raison de l'apparition de

la gestion de réseaux et de systèmes d'informatique répartis. La circulation d'informations à caractère personnel dans ce secteur repose pour une large part sur les liaisons et le réseau de télécommunication. Les lignes directrices énoncées au principe 8 s'appliquent à toutes les parties engagées dans des opérations de règlement - l'organisme fournissant des moyens de paiement et qui traite les données qui vont de pair avec son utilisation, le bénéficiaire de la transaction, les opérateurs techniques qui gèrent la transmission des données, les sous-traitants (qui peuvent aussi être les opérateurs techniques) qui peuvent exécuter certaines opérations de traitement au nom de l'organisme fournisseur, ainsi que les PTT qui fournissent des liaisons de télécommunications pour permettre à des activités comme les opérations de télébanking d'avoir lieu. Ainsi que le mentionne déjà le paragraphe 36, même si l'exploitant du réseau de communication ne procède ni à la collecte, ni à l'enregistrement ni au traitement des données à caractère personnel, il devrait néanmoins rester tenu d'assurer, dans la mesure du possible, les mesures structurelles et techniques mentionnées ci-dessous.

72. Les mesures structurelles et techniques adéquates évoquées au principe 8.1 doivent refléter l'état de la technique. Par exemple, il faut faire appel aux nouvelles techniques de codage et de cryptage pour préserver les données lorsqu'elles transitent par des liaisons de télécommunications. Les mesures de contrôle mentionnées au principe 8.2 peuvent revêtir diverses formes selon le rôle de l'acteur dans le traitement des données : contrôle de l'accès pour empêcher les personnes non autorisées à accéder à des systèmes informatiques traitant des données à caractère personnel; contrôle des supports de mémoire pour empêcher la lecture non autorisée des supports de mémoire ; contrôle de mémoire pour empêcher les entrées non autorisées dans les mémoires ainsi que toute manipulation non autorisée de données à caractère personnel enregistrées; contrôle de l'accès pour veiller à ce que les usagers autorisés désignés d'un système informatique ne puissent accéder à aucune autre donnée à caractère personnel que celles visées par leur droit d'accès; contrôle de l'entrée pour veiller à ce qu'il soit possible de contrôler et vérifier à quel moment et par qui les différents types de données à caractère personnel ont été traitées; contrôle des travaux pour s'assurer que les données à caractère personnel en cours de traitement par des sous-traitants ou des opérateurs techniques respectent les conditions fixées par l'organisme fournisseur; contrôle structurel pour s'assurer que le personnel des organismes fournissant des moyens de paiement, des bénéficiaires ainsi que des exploitants de réseaux de communication aient conscience des mesures de sécurité relatives aux données et de la nécessité de les respecter.

73. L'individu lui-même a un rôle à jouer dans la sécurité des données. Il doit prendre les mesures appropriées pour veiller à ce que son moyen de paiement ne tombe pas entre de mauvaises mains ou que des tiers n'apprennent son numéro de code ou PIN. La recommandation énoncée au principe 8.3 se retrouve déjà dans la pratique de certains organismes fournissant des moyens de paiement. Il est néanmoins considéré comme opportun de rappeler à quel point il importe que l'individu reçoive des instructions concernant la bonne gestion de son moyen de paiement et de ses codes.

9. Recours

74. Les recours visés au principe 9 peuvent figurer dans la législation interne relative à la protection des données. Ils peuvent être complétés par d'autres garanties prévues par le droit civil, pénal ou administratif. Dans certains pays, le secteur des services financiers est placé sous l'autorité d'organes régulateurs ou d'ombudsmen qui offrent à l'individu une voie de recours contre les activités des organismes fournissant des moyens de paiement. Il est néanmoins indispensable que de tels systèmes de contrôle permettent à l'individu d'attaquer

le refus des droits prévus au principe 7 ainsi que de contester toute violation d'un des autres principes énoncés dans la Recommandation.

10. Flux transfrontières de données

75. Ainsi qu'on l'a vu dans le Préambule de la Recommandation, les opérations de paiement ou autres opérations connexes peuvent avoir un caractère international. Il est de plus en plus fréquent qu'un moyen de paiement délivré dans un pays soit utilisé dans plusieurs autres. En même temps, les organismes fournissant des moyens de paiement peuvent traiter à l'étranger les données qu'ils collectent et enregistrent à la suite de l'utilisation d'un moyen de paiement. Le principe 10 de la Recommandation vise à fournir des lignes directrices sur la manière dont les données à caractère personnel peuvent circuler librement par-delà les frontières sans risque pour la vie privée de l'individu lorsqu'elles résultent de paiements ou d'autres opérations connexes. Le texte opère une distinction entre les flux de données selon qu'ils s'effectuent entre des Parties contractantes à la Convention sur la Protection des Données (principe 10.1) ou entre des Parties contractantes et non- contractantes (principe 10.2).

76. En ce qui concerne les Parties contractantes, celles-ci participent à une zone commune de protection des données du fait même qu'elles ont ratifié la Convention et qu'elles ont des normes internes sur la protection des données. En principe, aucun obstacle fondé sur la vie privée ne doit s'opposer à la circulation de données entre et parmi de tels Etats. L'intégrité et le caractère confidentiel des données collectées et enregistrées sur le territoire d'une Partie contractante à la suite de l'utilisation d'un moyen de paiement sont respectés dans l'Etat contractant où les données sont transférées par la suite. Cela dit, l'article 12 de la Convention sur la Protection des Données admet la possibilité pour une Partie contractante de déroger au principe de la libre circulation lorsque sa règlementation qui exige la communication des données n'assure pas une protection équivalente pour certaines catégories de données à caractère personnel ou de fichiers automatisés de données à caractère personnel. De la nature des données en question dépend la manière dont cette dérogation s'applique. Par exemple, les données peuvent être de caractère sensible. Il se peut que, pour certains pays, les données bancaires à caractère personnel relèvent de cette catégorie. C'est ce type de problème que résout le principe 10.1 de la Recommandation. Les rédacteurs de celle-ci ont estimé que la reconnaissance dans toutes les Parties contractantes des principes établis dans la Recommandation pouvaient assurer le niveau nécessaire de protection équivalente pour les données à caractère personnel utilisées à des fins de paiement et d'autres opérations connexes. Le terme "équivalente" ne saurait signifier identique. Le respect des principes figurant dans la Recommandation doit être suffisant pour assurer un degré équivalent de protection en vue d'assurer la libre circulation des données à caractère personnel utilisées à des fins de paiement ou d'autres opérations connexes.

77. En ce qui concerne la communication de données à caractère personnel entre une Partie contractante et une Partie non-contractante, la Recommandation encourage les autorités compétentes de toute Partie contractante à assurer la libre circulation des données vers les autres pays qui respectent les principes qu'elle contient. On rappelle qu'il y a des pays qui ont une législation sur la protection des données mais qui n'ont pas encore ratifié la Convention sur la protection des données. S'agissant de ces pays, le respect des principes figurant dans la Recommandation doit, selon les termes du principe 10.2, constituer "une forte justification pour permettre le transfert des données à caractère personnel vers [ces

Etats]". En effet, la Convention vise non seulement à protéger la vie privée de l'individu mais aussi à favoriser les flux transfrontières de données.

11. Conservation des données

78. Ni les organismes fournissant des moyens de paiement, ni les bénéficiaires, ni les exploitants de réseaux de communication n'ont intérêt à conserver des données à caractère personnel qui ne servent plus à rien. Le principe 11.1 recommande de ne pas conserver de données à caractère personnel plus longtemps que ne le nécessite l'accomplissement des diverses finalités prévues par les principes 3 et 4. Le texte s'efforce aussi de tenir compte du fait qu'il peut être nécessaire de conserver les données pendant un certain temps pour appuyer des actions en justice ou apporter la preuve de transactions réalisées par l'individu (principe 11.3). Par exemple, dans certains ordres juridiques, l'utilisation d'un moyen de paiement peut donner lieu à une relation débiteur-créancier-fournisseur qui permet au particulier de poursuivre en justice l'organisme fournissant le moyen de paiement lorsque les marchandises achetées chez un commerçant se révèlent défectueuses. En pareil cas, il est manifestement indispensable que l'organisme fournissant le moyen de paiement garde la trace de la transaction. Cela étant, les données ne devraient être conservées que pour une période raisonnable. C'est dans cette optique que le principe 11.3 de la Recommandation encourage les organismes fournissant des moyens de paiement à fixer des délais pour la conservation des données.

79. Le principe 11.3 traite aussi la question de savoir ce qu'il doit advenir des données à caractère personnel fournies par un individu dans l'espoir d'obtenir un moyen de paiement lorsque celui-ci est ensuite refusé. Dans ces conditions, il se peut que l'individu cherche à contester la décision - par exemple, en alléguant qu'il s'est vu refuser ce moyen de paiement pour des motifs fondés sur le sexe ou la race. L'organisme a besoin d'avoir le dossier des négociations avec l'individu qui s'estime lésé, pour pouvoir préparer sa défense. Cela étant, encore une fois, les données n'ont pas à être conservées indéfiniment. Il faut fixer des délais pour la conservation des données à caractère personnel lorsqu'un moyen de paiement a été refusé.

80. Le principe 11.2 de la Recommandation reprend la question du rôle du mandataire qui traite des informations pour le compte d'un organisme fournissant des moyens de paiement. En bref, une fois que le mandataire s'est acquitté de la tâche, toute donnée à caractère personnel en sa possession doit être effacée.

12. Contrôle du respect des principes

81. Le système de contrôle évoqué au principe 12.1 pourrait être constitué par les organes de contrôle créés en vertu de la législation nationale sur la protection des données. Les conditions d'enregistrement/de déclaration/d'autorisation que cette législation peut imposer aux utilisateurs de données pourraient favoriser la transparence souhaitée pour les organismes fournissant des moyens de paiement que préconise le principe 12.2. Le respect des principes contenus dans la Recommandation pourrait être encouragé par les autorités chargées de la protection des données en collaboration avec des associations représentatives des organismes fournissant des moyens de paiement. Pour assurer le respect des principes, ces associations représentatives pourraient engager un dialogue avec les autorités de surveillance en vue d'élaborer des codes de déontologie pour la protection des données à caractère personnel dans le secteur des moyens de paiement et d'autres opérations connexes.

82. Ainsi qu'il est dit plus haut dans le présent exposé, il arrive souvent que des organismes fournissant des moyens de paiement soient soumis au contrôle d'organes régulateurs ou d'ombudsmen chargés du secteur des services financiers. Ces types d'institutions sont considérés comme pouvant avoir un rôle précieux à jouer dans ce secteur s'agissant de favoriser le respect de la protection des données et plus particulièrement du type de principes figurant dans la Recommandation.