Exposé des motifs

Recommandation No.R (95) 4 du Comité des Ministres aux Etats membres sur la protection des données à caractère personnel dans le domaine des services de télécommunication, eu égard notamment aux services téléphoniques

(adoptée par le Comité des Ministres le 7 février 1995, lors de la 528e réunion des Délégués des Ministres)

Introduction

1. Les travaux du Conseil de l'Europe dans le domaine de la protection des données se sont toujours efforcés d'être technologiquement pertinents. Ainsi, les rédacteurs de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, du 28 janvier 1981 footnote 1, ont délibérément évité de geler la Convention en entrant dans les détails. La généralité de ses principes lui permet donc d'évoluer avec le temps. En outre, les recommandations sectorielles adoptées jusqu'ici par le Comité des Ministres, auxquelles il a été fait référence dans l'introduction, ont invariablement essayé d'aborder les nouveaux problèmes d'une manière technologiquement pertinente.

2. De même, le Groupe de projet sur la protection des données - c'est-à-dire les rédacteurs de ces instruments juridiques - a aujourd'hui porté son attention, dans cette recommandation, sur le secteur des télécommunications, et en particulier sur la téléphonie. Les risques que l'évolution des télécommunications entraîne pour la vie privée ont déjà fait l'objet d'un rapport qui a été établi par le groupe de projet et qui a ensuite été approuvé, en vue de sa publication, par le Comité des Ministres footnote 2. S'appuyant sur quelques-uns des thèmes exposés dans ce rapport, le groupe de projet s'est efforcé, dans la présente recommandation, d'apporter un certain nombre de principes directeurs pour garantir la vie privée de l'individu dans son utilisation des services de télécommunication et en particulier des nouveaux services téléphoniques. Cette fois encore, l'approche du groupe se veut technologiquement pertinente.

3. Tout en essayant de traiter certains des problèmes traditionnels qui ont longtemps caractérisé l'utilisation du téléphone, par exemple la vulnérabilité des communications téléphoniques aux ingérences ou interceptions illicites, les principes contenus dans la recommandation concernent essentiellement les problèmes nés de la numérisation des réseaux et des nouveaux services que cette évolution a permis.

4. Ces développements, évidemment, offrent d'énormes avantages aux abonnés et aux utilisateurs en général. La possibilité d'obtenir des factures détaillées est en effet intéressante pour les consommateurs, qui peuvent mieux maîtriser leurs dépenses en recherchant, grâce aux indications figurant sur la facture, la manière d'utiliser leur téléphone de façon plus économique. En outre, l'identification de l'appelant est un moyen de défense efficace contre les appels malveillants ou abusifs. Dernier exemple: les téléphones mobiles permettent aux hommes d'affaires en déplacement de rester en contact avec leur bureau.

5. Il convient toutefois de mettre ces avantages en balance avec les risques qu'ils entraînent pour la protection de la vie privée. Le groupe de projet a noté un certain nombre de caractéristiques des services qui exigent une réflexion attentive au niveau de la protection des données, de manière à assurer que leur introduction et leur utilisation s'inscrivent dans un environnement juridique approprié. En particulier, il est conscient du fait que certains de ces nouveaux services (comme l'identification de la ligne d'appel) génèrent des données à

caractère personnel lorsqu'ils sont utilisés, tandis que la numérisation des réseaux en général se traduira par l'augmentation des données enregistrées par les exploitants (comme l'illustre la possibilité d'obtenir des factures détaillées). Pour le groupe de projet, ces aspects du progrès peuvent non seulement menacer la vie privée des abonnés et des utilisateurs en général, mais également entraver leur liberté de communication, car ils diminuent le degré d'anonymat que les abonnés et utilisateurs peuvent souhaiter dans l'utilisation de leur ligne en les obligeant à révéler leur identité ou à laisser derrière eux des traces électroniques permettant de surveiller l'utilisation qu'ils font de leur terminal.

6. Les grands principes contenus dans la Convention s'appliquent, évidemment, à la collecte et au traitement des données à caractère personnel par les exploitants de réseaux et les exploitants de services de télécommunication dans les secteurs tant public que privé. Néanmoins, il a paru approprié d'offrir pour ce secteur des règles et directives spécifiques fondées sur les principes de la Convention, compte tenu des caractéristiques du secteur, notamment celles des nouveaux développements évoqués plus haut. Par exemple, il n'est pas d'emblée évident de savoir comment résoudre les nouveaux problèmes posés par l'identification de la ligne d'appel en se référant au texte de la Convention. Des solutions appropriées ne pourront être trouvées qu'à partir d'une analyse exhaustive de ce secteur. C'est alors seulement qu'il sera possible de déterminer la signification concrète des principes de "collecte loyale et licite", de "finalités déterminées" ou de sécurité des données, etc., contenus dans la Convention.

7. En outre, l'approche des rédacteurs de la recommandation est sous-tendue par d'autres normes fondamentales, s'ajoutant à celles énoncées dans la Convention. La recommandation se réfère fréquemment à l'article 8 de la Convention européenne des Droits de l'Homme et à la jurisprudence pertinente des organes de cette Convention. L'assimilation des données à caractère personnel traitées par les exploitants

de réseau dans la fourniture ou après l'utilisation d'un service de télécommunication ou de téléphone au principe du caractère privé de la correspondance garanti par l'article 8 est d'une importance particulière.

8. Enfin, un des grands principes contenus dans la Convention concerne la protection équivalente des données à caractère personnel qui font l'objet de transferts transnationaux. Il est évident que les développements des télécommunications conduisent à une communication internationale croissante des données à caractère personnel.

Au vu du caractère complexe de cette question - et des nombreux problèmes qui seraient soulevés pour tenter de réglementer, à ce stade, les flux transfrontières de données dans le secteur des télécommunications - les rédacteurs sont convenus de ne pas l'aborder dans le cadre de cette recommandation.

Préambule et dispositif

9. Les principes contenus dans la recommandation s'adressent à un certain nombre de parties.

10. En premier lieu, il est recommandé aux gouvernements des Etats membres de tenir compte des principes dans leurs législation et pratique internes. La législation sur la protection des données est un moyen évident pour l'expression de ces principes, en particulier à travers l'action des autorités établies en vertu de cette législation. C'est pourquoi le Comité des Ministres a demandé que la recommandation soit portée à leur attention. Les services chargés de la protection des données pourront trouver des solutions aux problèmes qu'ils rencontrent

dans ce secteur grâce à la recommandation. Après tout, cet instrument juridique a été établi par un comité de spécialistes à l'échelon international, à la lumière de l'analyse comparative des problèmes et des moyens appropriés pour les traiter. L'acceptation des diverses approches exposées dans la recommandation contribue également à réaliser "une union plus étroite entre les Etats membres du Conseil de l'Europe" dans le domaine de la protection des données.

11. Comme le reconnaît le dispositif de la recommandation, la législation relative à la protection des données n'est pas la seule forme législative permettant d'appliquer les principes. Les lois sur les télécommunications peuvent également s'acquitter de cette fonction. Qui plus est, la tendance à la réglementation sectorielle des questions relatives à la protection des données dans de nombreux pays suggère que cette méthode serait préférable, étant donné l'inaptitude des lois générales sur la protection des données à prévoir des règles détaillées pour tous les contextes de traitement privés et publics. Il faut toutefois signaler que, indépendamment du choix de la forme législative utilisée pour appliquer les principes, la compétence des services de protection des données pour traiter les problèmes se posant dans ce secteur reste inchangée.

12. La référence, dans le dispositif, aux "droit et pratique internes" permet une souplesse supplémentaire dans la mise en œuvre des principes proposés par la recommandation. Par exemple, les principes pourraient être consacrés dans des accords entre les gouvernements et les exploitants de réseau, qui octroient à ces derniers des concessions pour la fourniture et l'exploitation d'un réseau de télécommunication. Des codes de conduite peuvent être élaborés à l'intérieur des organes représentatifs du secteur concerné de manière à assurer le respect des principes dans la pratique industrielle. Toutefois, il faudra veiller soigneusement à ce que ces codes reçoivent l'approbation d'une autorité supérieure, par exemple d'un service responsable de la protection des données, ou d'un organe réglementaire du secteur des télécommunications.

13. En outre, le texte recommande également que les principes soient communiqués à un certain nombre d'acteurs clés dans ce secteur. La référence aux fournisseurs d'équipements et de logiciels s'explique par le fait que les principes encouragent l'exploitation d'équipements et de logiciels propres à réduire au minimum l'enregistrement de données à caractère personnel au moment de l'utilisation d'un service de télécommunication, notamment d'un service téléphonique. En particulier, les fournisseurs d'équipements et de logiciels devraient éviter de mettre sur le marché et d'exploiter commercialement des dispositifs ou accessoires téléphoniques qui constituent une atteinte à la vie privée de tierces personnes.

14. La référence aux organisations de consommateurs s'explique par le fait que les abonnés au téléphone appartiennent assez souvent à des groupes qui doivent être consultés par les exploitants de réseau. Les principes contenus dans la recommandation ont un impact assez évident sur les consommateurs. Ces groupes devraient s'efforcer de faire comprendre aux exploitants l'importance qu'il y a à donner effet aux principes.

15. Enfin, un certain nombre d'organismes internationaux sont compétents pour divers aspects de la politique des télécommunications. La normalisation est assez fréquemment déterminée à l'échelon international. La Commission européenne a récemment élaboré son propre ensemble de projets de directives pour assurer le respect de la vie privée dans les réseaux de télécommunication au sein des Etats membres de la Communauté. Etant donné la compétence spéciale du Conseil de l'Europe dans le domaine de la protection des données, il semble approprié de rappeler à ces forums l'importance et la pertinence de la présente recommandation.

Annexe à la recommandation

I. Champ d'application et définitions

16. Conformément au principe 1.1, le champ d'application de la recommandation englobe les exploitants de réseau et les fournisseurs de services dans les secteurs tant public que privé, ainsi que les autres organismes publics ou privés offrant des réseaux et/ou fournissant des services de télécommunication qui permettent la correspondance ou la communication entre utilisateurs.

17. Conformément à la Convention, les principes contenus dans la recommandation s'appliquent essentiellement aux données à caractère personnel qui font l'objet d'un traitement automatisé, tout en laissant aux Etats membres la possibilité de les étendre aux données à caractère personnel qui font l'objet d'un traitement manuel (principe 1.2). Il faut noter que certaines lois européennes sur la protection des données couvrent ces deux formes de traitement.

18. Ici encore, suivant l'exemple de la Convention, les Etats membres ont également la possibilité d'inclure les personnes morales dans le champ d'application de la recommandation et d'étendre les principes à la collecte et au traitement de données relatives aux sociétés, associations, etc. (principe 1.3). Comme dans le cas du traitement manuel des données, certains pays européens incluent dans leurs lois sur la protection des données les personnes morales et les personnes physiques.

19. La définition des "données à caractère personnel", au principe 1.4, a déjà été utilisée dans bon nombre de recommandations sectorielles adoptées par le Comité des Ministres dans le domaine de la protection des données. Cette fois encore, la définition est en conformité avec la Convention. Il va sans dire qu'un numéro de téléphone est une donnée à caractère personnel aux fins de la présente recommandation.

20. Ainsi qu'il a été noté plus haut, la numérisation des réseaux a créé une situation dans laquelle la ligne et le réseau de télécommunication peuvent être utilisés pour communiquer par message vocal, texte, image ou par transmission de données. En Europe, on s'oriente vers ce que l'on appelle le réseau numérique à intégration de services (RNIS). La numérisation des réseaux a amené les rédacteurs à éviter de trop axer la recommandation sur le téléphone au sens classique d'une communication vocale entre utilisateurs d'un téléphone. Limiter l'approche à la communication vocale aurait pour effet de négliger des questions telles que la transmission de textes ou d'images par fax. C'est pourquoi la recommandation se préoccupe de toutes les possibilités que les télécommunications offrent aujourd'hui aux utilisateurs. La définition des services de télécommunication pourrait même inclure le vidéotexte interactif, ou la télémétrie, ou la consultation électronique de bases de données, qui posent des problèmes similaires et exigent des solutions similaires. Cependant, la radiodiffusion et la télévision ne sont pas incluses dans cette définition.

21. L'exploitant de réseau est défini, dans le principe 1.4, comme l'organisme public ou privé qui fournit le réseau de manière à permettre aux abonnés et aux utilisateurs en général de correspondre et de communiquer par l'un des divers services mentionnés au paragraphe précédent. La fonction première de l'exploitant de réseau se limite à la fourniture et au fonctionnement du réseau, les services étant mis à disposition par un "fournisseur de services". Si l'exploitant de réseau fournit également les services en plus de la mise à disposition et de la gestion du réseau, les dispositions spécifiques aux fournisseurs de services s'appliquent aussi à lui.

22. Le texte reconnaît que les "fournisseurs de services" peuvent aussi exploiter leurs propres réseaux privés pour la communication et la correspondance par message vocal, texte, image ou par transmission de données. Alternativement, ces services peuvent être fournis par l'intermédiaire des grands réseaux offerts par les exploitants de réseau. La recommandation s'efforce donc d'englober à la fois les exploitants de réseau et les fournisseurs de services dans la mesure où ils collectent et traitent des données à caractère personnel aux fins de fournir et d'exploiter un réseau de télécommunication ou des services de télécommunication.

23. Les rédacteurs de la recommandation n'ont pas estimé nécessaire de définir l'expression "réseau de télécommunication" et se sont référés à la définition figurant dans d'autres textes internationaux pertinents.

24. Sans souhaiter le définir dans la recommandation, les rédacteurs sont convenus que le mot "utilisateur" désignerait l'utilisateur final des services de télécommunication, y compris, le cas échéant, d'autres exploitants de réseau et fournisseurs de services. De même, ils sont convenus que le terme "abonné" désignerait toute personne qui a conclu un contrat avec l'exploitant du réseau fournissant un service de télécommunication en vue de l'utilisation de ce service.

25. La recommandation n'emploie pas les expressions "données de base" ou "données de contenu", qui, dans l'industrie, se réfèrent respectivement aux données relatives à l'abonné et au contenu des communications. Le texte cherche à éviter la langue par trop technique, de manière à être facilement compréhensible. De même, les rédacteurs ont évité, au principe 4.5, d'utiliser l'expression "données de service". Cependant, ils sont convenus que, par "données de service", il fallait comprendre la totalité des données à caractère personnel générées par l'utilisation des services de télécommunication et enregistrées par l'exploitant du réseau à des fins techniques et opérationnelles, y compris à la prévention des abus et à des fins de facturation.

II. Respect de la vie privée

26. En plus du respect de la vie privée, le principe 2.1 recommande que les progrès réalisés dans le secteur des télécommunications ne constituent pas une entrave à la liberté de la communication. Les rédacteurs sont convenus que ce principe devrait s'appliquer à la fois aux utilisateurs et à leurs correspondants. Comme on le verra plus loin, les services téléphoniques tels que l'identification de la ligne d'appel ainsi que la fourniture de factures détaillées peuvent dissuader les abonnés ou les utilisateurs de communiquer par téléphone car ils tendent à constituer un danger pour l'anonymat. Les diverses dispositions de la recommandation essaient de minimiser les problèmes qui peuvent accompagner la révélation de données à caractère personnel au moment où l'on effectue des appels téléphoniques. En outre, le principe 2.2 essaye d'encourager les exploitants de réseau, les fournisseurs de services et les fabricants de matériel et de logiciels à imaginer des moyens d'accès anonymes aux réseaux de télécommunication. Par exemple, on pourrait instaurer un système fondé sur les télécartes préchargées utilisées dans les cabines téléphoniques publiques. Cette ligne d'action recommandée visant à accroître l'anonymat fait partie d'un thème plus général, à savoir la nécessité d'exploiter la technologie de l'information de manière à limiter la quantité de données à caractère personnel qui sont collectées et traitées par suite de l'utilisation du téléphone ou des services de télécommunication en général. Le principe 2.2 repose sur l'idée que, si l'adoption et l'utilisation de la technologie de l'information et en particulier la numérisation des réseaux ont accru la quantité de données à caractère personnel qui sont collectées et enregistrées, elles doivent également être en mesure de réduire au minimum la quantité des données enregistrées grâce à la mise au point d'une technologie respectueuse de la vie privée. Un aspect de cette question sera discuté dans le contexte du principe 7.16, à

savoir la nécessité d'élaborer des techniques pour supprimer l'affichage du numéro de la ligne d'appel sur le terminal de la personne appelée.

27. L'obligation pour les exploitants de réseau et les fournisseurs de services et d'équipement matériel et logiciel de garantir la protection de la vie privée des utilisateurs ne devrait pas être interprétée comme une interdiction, pour les Etats membres, de régler d'une façon ou d'une autre l'utilisation des algorithmes cryptographiques, afin de reproduire l'information d'origine dans un texte clair et compréhensible dans des cas où les télécommunications ont été interceptées sur ordre des autorités en vertu des règles en vigueur énoncées aux principes 2.4 et 4.2 et en tenant compte des garanties en question.

Par ailleurs, les rédacteurs de la recommandation ont accepté que les mesures prises conformément à ce principe devraient rendre possible d'effectuer une interférence légitime dans le contenu d'une communication conformément aux principes 2.3 et 2.4.

28. On notera que la protection envisagée dans la recommandation ne se limite pas aux abonnés des services de télécommunication ou de téléphone. Elle s'étend aux "utilisateurs" ainsi qu'aux "correspondants". Une référence aux utilisateurs se justifie par le fait que des problèmes ayant trait au respect de la vie privée se posent lorsque des non-abonnés, par exemple des personnes utilisant un central privé sur le lieu de travail, génèrent également des données de service. En ce qui concerne les correspondants, on verra que la présentation de factures détaillées aux abonnés peut avoir des incidences sur le plan du respect de la vie privée pour les personnes appelées par l'abonné. Pour ces raisons, il a été jugé nécessaire d'inclure les utilisateurs et les correspondants dans le système de protection.

La recommandation ne se réfère pas explicitement aux "co-utilisateurs" car dans la plupart des cas ils sont inconnus des exploitants de réseau et des fournisseurs de services, qui ne traitent qu'avec l'abonné.

29. Le cadre du système de protection envisagé dans la recommandation réserve un rôle clé à la notion classique du droit à la vie privée. Il faut se référer, en particulier, à la question de l'interception des communications qui est discutée aux principes 2.3 et 2.4, et qui s'inspire de la jurisprudence de la Cour européenne des Droits de l'Homme dans le contexte de l'article 8 de la Convention européenne des Droits de l'Homme. Aux fins de la présente recommandation, il importe de noter que le droit à la vie privée n'est pas la seule valeur soulignée par l'article 8 de la Convention européenne des Droits de l'Homme. La protection établie dans cette disposition s'étend également à la garantie du secret de la correspondance. Pour la Cour européenne des Droits de l'Homme, cette garantie doit s'appliquer aux conversations téléphoniques tout autant qu'au courrier. Le souhait de la Cour de rendre la Convention européenne des Droits de l'Homme technologiquement pertinente doit donc être considéré comme autorisant de placer la gamme complète des services de télécommunication qui permettent la communication ou la correspondance entre les abonnés ou les utilisateurs sous la protection énoncée à l'article 8 de la Convention européenne des Droits de l'Homme.

30. L'approche suivie dans cette recommandation est donc sous-tendue par deux ensembles de normes fondamentales combinées: d'une part, celles fixées dans la Convention et, d'autre part, les dispositions de l'article 8 de la Convention européenne des Droits de l'Homme.

31. Les principes 2.3 et 2.4 sont consacrés à l'inviolabilité des communications. Le principe 2.3 souligne l'illégalité de toute ingérence dans le contenu d'une communication par l'exploitant du réseau, à moins d'une autorisation de l'abonné ou pour des raisons légitimes. A titre d'exemple, l'exploitant du réseau peut être autorisé à lire des télégrammes par téléphone à

l'abonné ou à d'autres personnes autorisées par lui, ou, pour des raisons techniques, l'exploitant du réseau peut être tenu de regarder le message en vue de l'enregistrer ou de le transmettre à l'abonné. Cela peut être le cas des boîtes de courrier électronique.

32. Bien que la communication des données à des tiers fasse l'objet du chapitre 4, les rédacteurs de la recommandation ont jugé utile de préciser au principe 2.3 que les données relatives au contenu des messages, collectées en vertu de ce principe, ne devraient pas être communiquées à des tiers, sous réserve du principe 4.2.

33. Le principe 2.4, comme le principe 4.2, énonce des dispositions strictes calquées sur l'article 9 de la Convention et destinées à assurer un fondement juridique à l'ingérence des autorités publiques dans le contenu des communications, y compris l'ingérence à des fins de surveillance, pour identifier simplement l'abonné appelé. La Cour européenne des Droits de l'Homme, ainsi que mentionné plus haut, a déclaré à plusieurs reprises (par exemple dans les affaires Klass et autres, Malone, Kruslin et Huvig) que les pratiques telles que les enregistrements téléphoniques violaient le droit au respect de la vie privée et du secret de la correspondance garanti par l'article 8, paragraphe 1, de la Convention européenne des Droits de l'Homme. Toute dérogation à ce droit fondamental doit être en conformité avec le paragraphe 2 de l'article 8 de cette Convention.

34. Au principe 2.4, les références à l'utilisation des tables d'écoute ou à d'autres moyens de surveillance devraient être comprises comme s'appliquant à l'emploi des dispositifs ou d'autres moyens qui, de par leur nature, ont été désignés pour effectuer des ingérences dans les télécommunications, soit par interception, soit par d'autres moyens.

35. Quant à l'expression "est prévue par la loi", les rédacteurs de la recommandation l'entendent comme une référence au droit interne.

36. Le principe 2.5 tend à protéger les données de l'abonné dont la communication a fait l'objet d'une ingérence par des autorités publiques. Il est clair que dans le cas d'une ingérence dans les conditions énoncées au principe 2.4, les droits d'accès et de rectification de la personne concernée sont suspendus temporairement (article 9 de la Convention). Cependant, le droit interne devrait réglementer la possibilité pour la personne concernée d'exercer ses droits lorsque cette suspension prend fin. La loi devrait également indiquer les conditions dans lesquelles les autorités publiques concernées peuvent refuser l'accès (par exemple compromission des recherches, présence d'intérêts publics ou de tiers prépondérants), ainsi que les conditions dans lesquelles les données peuvent être conservées ou doivent être détruites.

37. Le principe 2.5 ne garantit pas à l'abonné le droit d'accès aux données le concernant et collectées par ingérence de la part des autorités publiques; le principe demande uniquement que le droit interne réglemente l'exercice de ce droit ainsi que les conditions dans lesquelles l'information de la personne concernée peut être refusée. Par exemple, le droit interne peut prévoir un système permettant à une personne de saisir une autorité judiciaire indépendante lorsqu'elle croit avoir fait l'objet d'une interception illégitime lors d'une télécommunication. Si l'autorité judiciaire parvient à la conclusion qu'il n'y a pas eu interception contraire à la loi, cette conclusion est notifiée à la personne sans préciser si oui ou non sa communication a été interceptée. Une telle procédure, à condition qu'elle prévoie un cadre de garantie contre toute utilisation arbitraire ou déraisonnable de pouvoirs statutaires à l'égard d'un individu dans sa position de requérant, a été acceptée par la Commission européenne des Droits de l'Homme, lorsqu'elle a déclaré "que la crainte des Etats, que l'efficacité d'un système puisse être compromise par l'information des requérants est légitime, et que l'absence de telle information

ne peut justifier en soi la conclusion que l'ingérence n'était pas nécessaire (c'est-à-dire dans une société démocratique)"1. (Requête no 21482/93, Christie contre le Royaume-Uni).

38. Par ailleurs, pour souligner l'inviolabilité des communications, même s'il y a eu ingérence, le principe 2.5 stipule que les données ainsi collectées ne devraient être communiquées qu'à l'organisme désigné dans l'autorisation pour cette ingérence. La communication de ces informations par l'organisme désigné ne relève pas de la présente recommandation.

39. Référence devrait également être faite aux principes énoncés dans la recommandation du Comité des Ministres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police (Recommandation no R (87) 15).

40. Le téléphone est malheureusement un moyen facile pour causer de la détresse aux abonnés. Les canulars aux services des urgences, les appels abusifs ou la simple communication de messages malveillants à des abonnés choisis au hasard sont les risques regrettables des services téléphoniques. Pour lutter contre ces types d'abus, le principe 2.6 prévoit la possibilité que des moyens techniques soient utilisés pour rechercher l'identité du coupable, en particulier lorsque les appels sont répétés et ne constituent pas un cas isolé. Les abonnés tourmentés par de tels appels peuvent demander qu'un appel entrant particulier soit surveillé en vue d'identifier la partie appelante. Dans certains pays, une autorisation judiciaire peut être nécessaire avant que la surveillance d'appel ne puisse être effectuée. Le droit interne devrait déterminer également le niveau de la preuve qui doit exister à l'égard d'une partie appelante particulière avant que ses appels ne puissent être surveillés. Il doit exister, au minimum, un soupçon raisonnable à son encontre.

41. A l'égard de l'expression "droit interne", les rédacteurs de la recommandation ont renvoyé au paragraphe 39 du rapport explicatif de la Convention:

"39. En fonction du système juridique et constitutionnel du pays concerné, les "mesures nécessaires dans son droit interne" peuvent revêtir, outre la loi, différentes formes telles que règlements, directives administratives, etc. De telles mesures contraignantes peuvent utilement être complétées par des mesures de réglementation volontaire dans le domaine de l'informatique, telles que des codes de bonne pratique ou des règles de conduite professionnelle. Toutefois ces mesures volontaires ne suffisent pas par elles-mêmes pour donner suite à la Convention."

42. On verra plus loin (principe 7.17) que l'une des raisons qui peut justifier l'exploitant du réseau à outrepasser la décision de l'abonné souhaitant supprimer son numéro et éviter son affichage sur le terminal de la partie appelée est l'identification de la source des appels abusifs ou malveillants.

III. Collecte et traitement des données

43. Les risques que les progrès réalisés dans ce secteur entraînent pour la vie privée ont déjà été évoqués dans le préambule. Il faut toutefois se souvenir que la protection de la vie privée ne se limite pas uniquement à préserver l'individu de l'ingérence des pouvoirs publics dans sa sphère personnelle. Il faut plutôt l'envisager sous l'angle des conditions dans lesquelles des informations à caractère personnel peuvent être licitement collectées et traitées par des tiers dans les secteurs tant public que privé. Cette nouvelle conception de la protection de la vie privée en termes d'autodétermination informationnelle, et qui est traduite, tout au long de la recommandation, par la nécessité d'assurer que l'abonné ou l'utilisateur se voie accorder des droits aux divers stades du traitement, explique la référence, au principe 3.1, à la Convention.

Ce traité international fournit la base du principe de l'autodétermination informationnelle tel qu'il doit être appliqué en droit national. Les dispositions de la recommandation ont pour but de préciser cette base dans le secteur considéré. En particulier, le principe de la Convention de la "détermination des finalités" (article 5.b) se voit précisé de manière à pouvoir être adapté aux réalités de la collecte et de l'enregistrement des informations par les exploitants de réseau et les fournisseurs de services. La recommandation identifie un certain nombre de finalités licites pour lesquelles des données à caractère personnel peuvent être collectées et traitées, à savoir:

- le raccordement d'un utilisateur au réseau: avant de s'abonner, il faut donner un certain nombre de renseignements à l'exploitant du réseau;

- la mise à disposition d'un service de télécommunication déterminé: cela peut exiger la publication de certaines données dans un annuaire;

- la facturation et la vérification: cela impliquera la collecte et le traitement de données concernant la ligne appelée, celle à partir de laquelle l'appel a été effectué, la durée de la communication, etc. L'exploitant de réseau peut avoir également besoin de traiter des données relatives aux abonnés qui ne paient pas leur facture;

- la nécessité d'assurer une opération technique optimale du réseau

et du service: par exemple, il peut être nécessaire d'enregistrer des données de manière à déterminer le volume du trafic de correspondance à des périodes particulières, ou à réparer des erreurs;

- le développement du réseau ou des services: cela peut exiger la collecte et le traitement de données.

44. Comme dans le cas des personnes concernées par des données en général, les abonnés aux services de télécommunication, y compris aux services téléphoniques, ne devraient pas être exclus du circuit de l'information. Les données collectées et traitées par des tiers les concernent. En conséquence, ils ont le droit de savoir autant que possible quelles sont les données qui seront collectées et traitées, la base juridique sur laquelle cela sera fait, les fins auxquelles elles seront collectées, les utilisations qui en seront faites et leur durée de conservation. Afin de rendre ce principe effectif, il est nécessaire d'introduire une certaine transparence dans les activités informationnelles des exploitants de réseau et des fournisseurs de services. Tel est l'objectif du principe 3.2, qui reflète, en fait, la nécessité de collecter et de traiter les données à caractère personnel loyalement et licitement (article 5.a de la Convention).

45. Conformément aux dispositions du principe 3.2, les exploitants de réseau et les fournisseurs de services devraient informer leurs abonnés des éléments suivants:

i. Les catégories de données à caractère personnel qui sont collectées et traitées

Par exemple, l'abonné devrait être informé du fait que l'exploitant de réseau enregistre les données qu'il a fournies au moment de sa demande de raccordement au réseau. En outre, il devrait être informé du fait que l'exploitant de réseau collecte et traite certaines données au moment où la communication est établie, à savoir le numéro appelé et la durée de l'appel. De plus, il devrait être informé que les données qui figurent dans l'annuaire (qui peuvent ne pas être les mêmes que celles fournies lors de la demande du service de télécommunication ou de téléphone) sont également enregistrées par l'exploitant de réseau.

ii. Les bases juridiques de la collecte

L'abonné devrait être informé du texte juridique en vertu duquel ses données sont collectées.

iii. Les principales finalités pour lesquelles les données à caractère personnel sont collectées et traitées

Pour satisfaire à cette exigence, l'exploitant de réseau ou le fournisseur de services devrait informer l'abonné que les données de service ne sont collectées et traitées que pour permettre de lui envoyer une facture. En ce qui concerne les données à caractère personnel fournies par l'abonné au moment où il demande un service téléphonique, l'exploitant de réseau devrait clairement indiquer que ces données sont simplement enregistrées pour permettre à l'abonné de bénéficier du service et d'être raccordé au réseau, et éventuellement pour assurer qu'il n'essaie pas de se réabonner sous un faux nom de manière à dissimuler le fait qu'il n'a pas payé ses factures.

iv. L'utilisation qui est faite des données

L'abonné devrait être clairement informé du fait que toute utilisation s'écartant des objectifs licites indiqués sous ii requiert une autorisation de sa part. Par exemple, lorsqu'on essaye d'utiliser les données de base à des fins de sollicitation commerciale, les garanties énumérées aux principes 7.7 à 7.11 devraient être invoquées.

La "manière appropriée" dont ces informations peuvent être fournies va de leur indication dans le contrat initial entre l'abonné et l'exploitant de réseau à la possibilité de les inclure dans l'annuaire téléphonique. En outre, les exploitants de réseau ou les fournisseurs de services pourraient rappeler aux abonnés les facteurs énumérés au principe 3.2 au moment où ils leur envoient la facture.

46. Les informations évoquées dans ce principe devraient également aller jusqu'à porter à l'attention des abonnés les droits évoqués au principe 5.1, la manière et les moyens de les exercer.

47. Pour les raisons énoncées au paragraphe 37 ci-dessus, il est clair que le principe 3.2 ne s'applique pas aux données à caractère personnel qui ont été collectées par les exploitants de réseau et les fournisseurs de services conformément aux principes 2.4 et 2.5.

IV. Communication des données

48. Les principes 4.1 à 4.4 de la recommandation énoncent un certain nombre de lignes directrices qui visent à réglementer les circonstances dans lesquelles les données à caractère personnel, que ce soit des données de contenu, des données de service ou des données de base, peuvent être communiquées à des tiers.

Le principe 4.1 énonce la règle générale selon laquelle aucune donnée à caractère personnel ne devrait être communiquée sans le consentement écrit de la personne concernée, ou lorsque cette communication pourrait conduire à l'identification de l'abonné appelé.

Le principe 4.2 énumère les conditions qui doivent être remplies avant que des données à caractère personnel ne puissent être communiquées à des autorités publiques.

Le principe 4.3 indique les différents aspects qui doivent être réglementés par le droit interne pour la communication de données à caractère personnel à des autorités publiques.

Le principe 4.4 concerne la situation relative à la transmission de listes d'abonnés à des tiers à toute fin légale, y compris de marketing direct, et est dans ce sens lié aux principes 7.7 à 7.11.

Le principe 4.5, enfin, traite de la communication de données à caractère personnel entre exploitants de réseau et fournisseurs de services.

49. Les données de contenu ne devraient en principe pas être collectées par les exploitants de réseau et les fournisseurs de services, sauf dans les cas exceptionnels définis aux principes 2.3 et 2.4.

50. Les circonstances dans lesquelles les données de service peuvent être communiquées à des organismes privés ou à des personnes seront rares. Il est toutefois possible d'imaginer des demandes de communication de données de service émanant de sociétés de recherche en train d'analyser l'utilisation faite des services téléphoniques ou d'autres services de télécommunication dans des localités données. Le principe 4.1 exige que l'abonné donne son consentement exprès et éclairé par écrit pour que ses données de service puissent être communiquées à de tels organismes. En outre, étant donné que les données de service peuvent révéler l'identité des correspondants d'un abonné, il est nécessaire d'assurer que les données à communiquer ne permettent pas que ces identités puissent être déterminées. Dans ce souci, il conviendrait d'utiliser des techniques d'anonymisation pour cacher l'identité des abonnés qui ont été appelés à partir du terminal de l'abonné.

51. La personne concernée peut retirer son consentement mais, pour des raisons évidentes, le retrait est sans effet rétroactif.

52. Comme on le verra au principe 7.13, les données de service pour facturation devraient être effacées par l'exploitant de réseau après le paiement de la note téléphonique par l'abonné.

53. On a fréquemment relevé, au cours du présent commentaire, qu'une prudence particulière s'impose lorsqu'on détermine les conditions régissant l'utilisation et la communication des données de service. De par leur nature, les données de service sont révélatrices de situations humaines: ainsi, elles révèlent la ligne à partir de laquelle l'appel a été effectué, l'heure de la communication et sa durée, ainsi que le numéro de la ligne appelée. C'est pourquoi les rédacteurs de la recommandation ont essayé de placer les données de service sous la protection du principe fondamental du caractère privé de la correspondance ou des communications tel qu'énoncé à l'article 8 de la Convention européenne des Droits de l'Homme et reflété dans l'article 9 de la Convention. Il importe de noter que la Cour européenne des Droits de l'Homme a, par son interprétation évolutive de l'article 8, statué que la communication de telles données à l'insu de l'abonné doit être en conformité avec les strictes dispositions du paragraphe 2 de l'article 8. Or, dans l'arrêt rendu par la Cour dans l'affaire Malone, il est dit:

"(...) La Cour ne considère pas pour autant que l'exploitation des éléments rassemblés de la sorte [c'est-à-dire par le moyen du comptage] ne puisse jamais poser de problème sur le terrain de l'article 8. Dans un relevé ainsi dressé figurent des informations - notamment les numéros composés - qui font partie intégrante des communications téléphoniques. Aux yeux de la Cour, les révéler à la police sans l'accord de l'abonné porte donc aussi atteinte à un droit consacré par l'article 8."1

54. C'est pour cette raison que le principe 4.2 reprend le libellé du paragraphe 2 de l'article 9 de la Convention. En conséquence, la communication de données de service aux autorités publiques sans le consentement de l'abonné doit:

a. être prévue par la loi telle qu'interprétée par la Cour européenne des Droits de l'Homme dans des affaires telles que l'affaire Malone;

b. constituer une mesure nécessaire au sens de l'interprétation de la Cour des Droits de l'Homme dans l'affaire Malone et être dans l'intérêt de l'un des facteurs énoncés dans le principe 4.2.

55. Les rédacteurs de la recommandation sont convenus que le principe 4.2 n'empêche pas la communication de données à caractère personnel entre exploitants de réseau ou fournisseurs de services et une autorité de contrôle, lorsque cette communication est nécessaire à l'autorité concernée pour exercer ses fonctions selon le droit interne.

56. Les exploitants de réseau et les fournisseurs de services pourraient communiquer des données, selon les conditions énoncées dans l'article 9 de la Convention, aux autorités publiques, mais non aux organismes publics.

57. En outre, la recommandation exige, au principe 4.3, que le droit interne réglemente un certain nombre d'aspects lorsque les données à caractère personnel sont communiquées à des autorités publiques: l'exercice des droits d'accès et de rectification, le refus des autorités publiques de donner des renseignements à la personne concernée, et la conservation ou la destruction des données communiquées aux autorités publiques.

58. Dans le principe 4.3, les références aux droits d'accès et de rectification et aux conditions dans lesquelles les autorités publiques compétentes sont habilitées à refuser l'information de la personne concernée doivent être comprises comme permettant le refus des droits d'accès et de rectification lorsque cela est prévu par le droit et constitue une mesure nécessaire, dans une société démocratique, à la sécurité de l'Etat, à la sécurité publique, aux intérêts monétaires de l'Etat ou à la répression des infractions pénales.

59. Le principe 4.4 admet que les listes d'abonnés, c'est-à-dire les listes des données de base traitées par les exploitants de réseau et les fournisseurs de services de tous les abonnés - sans tenir compte de leur inclusion dans un annuaire - ne peuvent être communiquées à des tiers pour toute finalité (légale), non seulement à des fins de marketing direct mais aussi pour des sondages d'opinion, des statistiques, des enquêtes, des études de marché, etc., que si l'une des conditions énumérées est remplie. Les rédacteurs de la recommandation reconnaissent que ces conditions peuvent se chevaucher, dans une certaine mesure, mais soulignent qu'elles sont alternatives et non cumulatives.

60. De telles listes d'abonnés constituent une source précieuse de données à caractère personnel pour, notamment, des finalités de marketing direct. Les informations qu'elles contiennent peuvent servir à enrichir d'autres fichiers, afin d'obtenir une vue plus précise des populations de consommateurs potentiels, pour des produits ou services donnés. L'existence d'annuaires enregistrés sur CD-Rom ou sur des moyens magnétiques et la technique de télédéchargement ouvrent aux firmes de marketing des possibilités accrues de cibler leurs clients potentiels, en reliant les données à d'autres fichiers ou simplement en recherchant par des moyens automatisés des listes de noms qui tendent à révéler certaines caractéristiques des abonnés, comme leur nationalité ou leur groupe d'âge. Cette dernière possibilité comporte évidemment de graves risques pour la vie privée, car elle permet la création de profils par l'interconnexion de différents ensembles de données et l'exploitation de données à caractère personnel en dehors de leur contexte licite. Les simples noms et adresses ou numéros de téléphone ne peuvent pas non plus être considérés comme des données anodines pour la vie privée. Le fait que les noms permettent d'identifier la nationalité ou l'origine ethnique, surtout

si on peut les regrouper automatiquement, rend essentiel le fait de déterminer les conditions régissant leur utilisation par des tiers.

61. Compte tenu de ces considérations, le principe 4.4 s'efforce de subordonner la communication de données relatives aux abonnés au respect de certaines sauvegardes. Le principe 4.4 s'inspire du point de vue adopté dans la précédente Recommandation du Comité des Ministres relative à la protection des données à caractère personnel utilisées à des fins de marketing direct (Recommandation no R (85) 20) ainsi que de la recommandation sur la communication à des tierces personnes de données à caractère personnel détenues par des organismes publics (Recommandation no R (91) 10). Le texte du principe 4.4 reconnaît que la communication de listes d'abonnés, notamment par des moyens télématiques ou par une délivrance de bandes magnétiques, peut être subordonnée à l'une des conditions suivantes:

a. obtention du consentement exprès et éclairé, par écrit, de l'abonné; ou,

b. indication à celui-ci, au moment de la conclusion du contrat initial avec l'exploitant de réseau, qu'il peut s'opposer à la communication de ses données à des tiers à des fins de marketing direct et que, en vue de cela, il peut se faire inscrire sur une liste échappant à la publicité (liste orange); ou

c. autorisation de l'autorité chargée de la mise en œuvre et de l'application de la législation relative à la protection des données; ou

d. disposition correspondante du droit interne.

Le principe 4.4 offre ces divers degrés de sauvegardes alternatives et non cumulatives de manière à refléter la situation dans les différents Etats membres du Conseil de l'Europe.

62. Les dispositions du principe 4.5 autorisant la communication de données de service entre exploitants de réseau et fournisseurs de services pour les finalités qui y sont mentionnées sont une simple reconnaissance du besoin occasionnel de coopération technique entre différents exploitants de réseau et fournisseurs de services, afin de permettre l'exécution d'appels téléphoniques.

V. Droits d'accès et de rectification

63. Le principe 5.1 reprend les droits mentionnés à l'article 8 de la Convention. Pour permettre l'exercice effectif des droits d'accès et de rectification, les exploitants de réseau et les fournisseurs de services devront faire en sorte que les données qu'ils détiennent sur les abonnés puissent être facilement retrouvées lorsqu'on souhaite y accéder. En conséquence, si les informations se trouvent dans différents fichiers, il faudrait pouvoir rassembler la totalité des données.

64. L'accès aux données détenues par les exploitants de réseau ou les fournisseurs de services présente un intérêt essentiel pour les abonnés qui ne désirent pas qu'une facture détaillée leur soit adressée. Le principe 5.1 leur permettra d'obtenir de l'exploitant de réseau ou du fournisseur de services une liste des appels qu'ils ont effectués, de manière à pouvoir vérifier l'exactitude de leur note téléphonique.

65. La recommandation attache une grande importance à l'exercice par l'abonné des droits d'accès à ses données à caractère personnel et de rectification de ces données en raison également du fait que les exploitants de réseau et les fournisseurs de services peuvent, en vertu des principes 2.3 et 2.4, collecter des données de contenu. Les conditions auxquelles

l'accès aux données à caractère personnel et/ou la rectification de ces données peuvent être refusés, restreints ou différés par les exploitants de réseau ou les fournisseurs de services sont donc énoncées au principe 5.2 et correspondent aux dispositions strictes de l'article 9 de la Convention.

66. Les rédacteurs de la recommandation sont convenus toutefois que les demandes d'accès aux données à caractère personnel ne pourront pas toujours être satisfaites si ces demandes doivent occasionner aux exploitants de réseau ou aux fournisseurs de services des délais ou des activités déraisonnables.

VI. Sécurité

67. La sécurité des données est une composante principale de la politique de protection des données. Tandis que les principes précédents se proposent de traiter de la question de la vulnérabilité de l'individu eu égard à la collecte et au traitement des données à caractère personnel dans ce secteur, les principes 6.1 et 6.2 sont consacrés à la vulnérabilité des systèmes. Ces principes sont calqués sur l'article 7 de la Convention. La responsabilité incombe à l'exploitant de réseau de prendre les meilleures mesures possibles pour assurer la sécurité du réseau contre les menaces d'ingérence non autorisée dans la transmission des messages, ou d'ingérence non autorisée ou d'accès aux différentes catégories de données enregistrées. Des consignes claires devraient être données au personnel sur l'importance de respecter les données et la sécurité du réseau, et il devrait être formé dans la manière d'y parvenir. En outre, il devrait être instruit sur l'importance de maintenir le principe du secret des communications.

68. Concernant la sécurité des données, les facteurs suivants devraient être pris en considération: contrôle de l'accès pour empêcher les personnes non autorisées d'accéder aux systèmes informatiques traitant des données à caractère personnel; contrôle du moyen d'enregistrement pour empêcher la lecture non autorisée des moyens d'enregistrement; contrôle de la mémoire pour empêcher toute divulgation non autorisée ou toute manipulation non autorisée des données à caractère personnel enregistrées; contrôle de l'accès pour assurer que les utilisateurs désignés autorisés à accéder à un système de traitement ne puissent accéder aux données à caractère personnel autres que celles auxquelles leur droit d'accès se réfère; contrôle des informations fournies afin qu'il soit possible de contrôler et de vérifier à quel moment et par quelle personne les différentes catégories de données à caractère personnel ont été traitées; contrôle organisationnel pour assurer que le personnel est conscient des mesures de sécurité des données et de la nécessité de les respecter.

69. Concernant l'ingérence ou la surveillance des communications en cours de transmission, les exploitants de réseaux devraient assurer la sécurité des lignes de télécommunication et du réseau en général.

70. Les abonnés devraient être informés du rôle qu'ils peuvent jouer dans la mise en œuvre de la politique de sécurité. Comme cela a déjà été noté plus haut en ce qui concerne les téléphones mobiles, si les techniques de chiffrement sont disponibles, les abonnés aux téléphones mobiles devraient les utiliser. En outre, les abonnés aux télécopieurs devraient éviter d'envoyer des messages sensibles par l'intermédiaire de fax. Lorsque les messages laissés sur des répondeurs téléphoniques peuvent être écoutés à distance, les abonnés devraient assurer la sécurité des interrogations à distance. Les boîtes de courrier électronique devraient être protégées par des codes d'accès ou des cartes à puce gérés en toute sécurité par l'abonné.

VII. Application des principes

a. Annuaires

71. Les principes 7.1 à 7.6 concernent les garanties qui devraient accompagner la confection et l'utilisation des annuaires informatisés produits par les exploitants de réseau et les fournisseurs de services dans l'accomplissement de leurs fonctions, y compris la version imprimée de ces annuaires. Bien que ces principes se rapportent essentiellement aux annuaires téléphoniques, il faut se souvenir que le développement des services de télécommunication a entraîné l'apparition de toute une série d'annuaires supplémentaires destinés aux abonnés; par exemple, la popularisation des téléphones mobiles et des télécopieurs a donné naissance à des annuaires spécifiques à ces services. La recommandation vise en particulier les annuaires téléphoniques car ils constituent la principale source de données à caractère personnel qui soit accessible au public. C'est précisément la facilité de consultation des listes des abonnés au téléphone ainsi que l'existence de telles listes sous forme tant manuelle qu'automatisée qui a conduit les rédacteurs de la recommandation à envisager un certain nombre de garanties pour les abonnés.

72. En outre, la tendance accrue à utiliser les données relatives aux abonnés comme base pour des stratégies commerciales et de marketing, notamment par les exploitants de réseau eux-mêmes, est précisément l'une des raisons qui a conduit les rédacteurs de la recommandation à mettre en avant le principe 7.1, à savoir le droit pour l'abonné de ne pas figurer dans l'annuaire. Il y a d'autres raisons pour lesquelles on peut souhaiter disposer de ce droit, en dehors du simple désir d'éviter le harcèlement commercial, que ce soit par téléphone ou par courrier postal. La crainte d'appels malveillants ou abusifs est également une raison fréquemment invoquée pour ne pas figurer dans l'annuaire. Ou encore, il peut s'agir d'un simple désir de préserver son anonymat.

73. Ces considérations ont amené les rédacteurs de la recommandation à définir une solution idéale vers laquelle les gouvernements devraient tendre: le droit de chaque abonné d'être exclu de l'annuaire, à sa demande, sans versement d'une redevance et sans avoir à justifier sa demande. Ce principe repose sur la conviction que la possibilité d'être exclu de l'annuaire n'est pas un service fourni par l'exploitant de réseau, mais un moyen qui doit être librement accessible au particulier pour qu'il puisse protéger sa vie privée et sauvegarder son anonymat.

74. Si le premier alinéa du principe 7.1 énonce l'objectif désiré, les deux alinéas suivants essaient de conduire les Etats qui ont des règles différentes à se rapprocher de cet objectif en réduisant au minimum les restrictions apportées à l'exercice du droit en question.

75. Premièrement, lorsque l'abonné est légalement tenu de donner certains détails concernant sa ligne dans l'annuaire, il devrait néanmoins avoir la possibilité d'être dispensé de l'obligation de prouver, de façon satisfaisante pour l'exploitant du réseau, que la publication de son nom et de son numéro aurait des conséquences nuisibles pour lui - par exemple qu'il serait exposé à des appels abusifs - ou que la nature de son activité professionnelle exige la préservation de son anonymat.

76. Deuxièmement, dans les pays où un paiement est exigé d'un abonné qui souhaite que ses données ne soient pas incluses dans l'annuaire, ce paiement devrait être d'un montant raisonnable et dans les moyens de tout abonné souhaitant faire usage de cette possibilité. On peut noter à ce propos que les exploitants de réseau justifient parfois la perception d'un droit en arguant que l'augmentation du nombre des abonnés souhaitant ne pas figurer dans l'annuaire impose une charge supplémentaire au service des renseignements. Cette

justification perdra, semble-t-il, beaucoup de sa substance au fur et à mesure que l'on s'orientera vers l'adoption d'annuaires électroniques, qui permettront aux services de fonctionner beaucoup plus rapidement.

77. Comme il a été noté plus haut, les principes contenus dans cette recommandation ne se limitent pas simplement à assurer la protection des abonnés. La recommandation se préoccupe également d'étendre les garanties aux utilisateurs. Un problème particulier, s'agissant des listes d'abonnés, est celui des co-utilisateurs du terminal d'un abonné principal. L'abonné principal peut souhaiter que leurs nom et adresse (et éventuellement d'autres informations) figurent dans l'annuaire. Conformément au principe 7.2, tout abonné souhaitant le faire doit prouver de manière satisfaisante pour l'exploitant du réseau que les co-utilisateurs de son terminal (par exemple, les membres adultes de sa famille, ou les personnes partageant des locaux sous la responsabilité de l'abonné) ont donné leur consentement à leur inclusion dans l'annuaire.

78. Quelle quantité de données peut-on demander à l'abonné en vue de les inclure dans l'annuaire? Si l'article 5.b de la Convention stipule que les données à caractère personnel collectées et enregistrées ne doivent pas être excessives par rapport à l'objectif en question, le principe 7.3 interprète cette disposition comme signifiant, dans le contexte des données relatives à l'abonné, que les données à publier devraient être nécessaires et suffisantes pour remplir l'objectif d'un annuaire, à savoir permettre au public de trouver le numéro de téléphone d'un abonné à partir de son nom. A cette fin, et compte tenu du droit recommandé pour les abonnés de ne pas figurer dans l'annuaire, les données à publier devraient être limitées au nom, éventuellement aux prénoms, de manière à éviter la confusion avec des abonnés ayant le même nom de famille, avec la possibilité de mentionner simplement les initiales du prénom, le nom de la rue et éventuellement seulement le code postal. Cependant, la publication du nom et de l'adresse complète ne peut être exclue si cela est conforme au droit et à la pratique internes. Les exploitants de réseau devraient être sensibles à la nécessité de respecter le souhait de certains abonnés, à savoir que leur prénom ne soit pas publié. Le principe 7.3 admet que tout abonné peut exprimer le souhait de voir d'autres détails personnels figurer dans l'annuaire, par exemple ses diplômes, titres ou qualifications professionnelles.

79. Les rédacteurs de la recommandation ont reconnu que l'expression "données nécessaires à identifier raisonnablement" devrait être interprétée à la lumière des pratiques existantes, qui pourraient varier d'un pays à un autre. Dans certains cas, l'adresse d'un abonné peut, à sa demande, être incluse dans un annuaire si cela constitue une solution raisonnable pour résoudre un problème d'homonymie.

80. En ce qui concerne les annuaires électroniques, le principe 7.4 recommande que des moyens techniques soient mis en place pour prévenir les abus et notamment les télédéchargements non autorisés, et une restriction à la pratique des appariements.

81. Les rédacteurs de la recommandation ont également été conscients de la relation entre les principes 4.3 et 7.4. Cependant, alors que le principe 4.3 réglemente la communication aux autorités publiques de listes complètes d'abonnés, il ressort clairement du principe 7.4 que celui-ci ne s'applique qu'à un service rendu par les exploitants de réseau et les fournisseurs de services: fournir une information ponctuelle en réponse à des demandes précises, et uniquement concernant les données qui figurent dans l'annuaire. Le droit interne devrait organiser des mesures pour éviter les abus dans l'utilisation des services de renseignements relatifs aux annuaires.

82. Les personnes n'ayant pas directement accès à un annuaire électronique peuvent essayer de trouver le numéro de téléphone de leur correspondant en s'adressant au service des renseignements téléphoniques. En vertu du principe 7.5, pour autant que le numéro recherché ne soit pas exclu de l'annuaire, ce service peut le communiquer. Dans certains pays, il est possible au service des renseignements de se mettre en rapport avec un abonné ne figurant pas dans l'annuaire pour lui demander s'il désire que son numéro soit communiqué en réponse à une demande. Ce peut être le cas lorsque l'auteur de la demande d'information insiste pour obtenir le renseignement demandé. Dans ce type de situation, la décision finale de communiquer le numéro appartient à l'abonné et non au service.

83. Le service des renseignements peut-il communiquer davantage que le simple numéro d'un abonné, par exemple son adresse ou tout autre détail qui figure dans l'annuaire publié? L'annuaire est une méthode commode et pratique de s'informer sur l'adresse d'une personne, même sans intention de lui téléphoner. La situation est-elle différente lorsque l'information est demandée par l'intermédiaire du service des renseignements? Les rédacteurs de la recommandation ont reconnu qu'il faut éviter les abus et, par exemple, ne pas donner des renseignements lorsque le requérant ne connaît pas le nom de la personne recherchée. Toutefois, le service de renseignements doit pouvoir donner des informations identiques à celles figurant dans l'annuaire papier ou électronique (égalité de traitement entre les personnes ayant un vidéotex ou un minitel à leur disposition et celles qui doivent recourir au service de renseignements).

84. Le principe 7.6, enfin, se réfère aux dispositions de la Recommandation no R (91) 10 sur la communication à des tierces personnes de données à caractère personnel détenues par des organismes publics. Afin de tenir compte des problèmes que cette référence peut soulever pour les Etats dans lesquels les annuaires du téléphone ne sont pas considérés comme des fichiers publics et pour les Etats qui ont émis des réserves dans le cadre de la Recommandation no R (91) 10, la référence est limitée "aux principes pertinents" de la Recommandation no R (91) 10.

b. Utilisation des données à des fins de marketing direct

85. Les principes 7.7 à 7.11 s'appliquent à toutes les formes de marketing direct, y compris non seulement la sollicitation commerciale, mais également la sollicitation politique et les démarches effectuées par les syndicats, les associations caritatives, etc.

86. Comme exposé ci-dessus, le principe 4.4 cherche à prévoir des lignes directrices sur les conditions et sauvegardes qui devraient régir la communication de listes d'abonnés à des tierces personnes à toute fin légitime y compris de marketing direct, sondages d'opinion, enquêtes statistiques, études de marché. Il est à noter que l'approche s'inspire des dispositions de la Recommandation no R (85) 20 relative à la protection des données à caractère personnel utilisées à des fins de marketing direct. Les principes 7.7 à 7.11, qui traitent de l'utilisation de telles données à des fins de marketing direct, s'inspirent également de cette même recommandation et, en fait, s'y réfèrent. Bien que la Recommandation no R (85) 20 vise spécifiquement le télémarketing, il a été estimé nécessaire de prévoir des lignes directrices additionnelles sur la manière de minimiser les risques pour la vie privée qui accompagnent cette pratique commerciale par voie de télécommunication, étant donné qu'il s'agit d'une pratique qui a évolué en tant que technique depuis l'adoption de la recommandation antérieure.

87. En ce qui concerne la façon dont les données d'abonnés peuvent être utilisées par des tiers à des fins de marketing direct, les sociétés de marketing, les sociétés de vente par

correspondance, etc., devraient garder à l'esprit que les abonnés disposent de certains droits à l'égard des listes de marketing établies sur la base d'informations contenues dans les annuaires ou communiquées par des exploitants de réseau conformément aux dispositions du principe 4.4. En premier lieu, les abonnés peuvent, à tout moment, sur demande, faire effacer ou faire enlever leurs données sur les listes de marketing détenues par les utilisateurs. De plus, ils disposent du droit d'obtenir et de faire rectifier les données les concernant contenues sur des listes ou des fichiers de marketing direct. En outre, des mesures appropriées devraient être prises afin que les abonnés puissent exercer ces droits et identifier le maître du fichier du marketing. D'autres principes pertinents sont prévus dans la Recommandation no R (85) 20.

88. Il va sans dire que les abonnés jouissent du droit de ne pas faire inclure leurs données dans les annuaires, conformément aux dispositions de la Recommandation no R (85) 20. Ils devraient également disposer du droit de se faire inscrire sur des listes oranges (listes échappant à la publicité), qui indiquent à l'exploitant du réseau qu'ils ne souhaitent pas recevoir de matériel publicitaire ou promotionnel. Le principe 4.4 énumère un nombre de sauvegardes protectrices additionnelles qui permettent aux abonnés d'empêcher que leur nom soit inclus dans des listes de marketing. Tous ces éléments devraient être respectés lorsque des sociétés de marketing ou de vente par correspondance cherchent à exploiter des données d'abonnés. Ce facteur revêt une grande importance, étant donné que la Recommandation no R (85) 20 permet à toute personne "de collecter des données à caractère personnel à des fins de marketing direct à partir de fichiers ouverts au public ou d'autres matériels publiés". Comme il a été noté à un stade antérieur, les annuaires constituent l'un des fichiers publics les plus importants. Néanmoins, le fait que l'annuaire téléphonique soit accessible au public ne signifie pas que les données nominatives qui y sont contenues ne devraient pas faire l'objet d'une protection. Cela explique la raison pour laquelle le principe 2.2 de la Recommandation no R (85) 20 envisage de prévoir, dans le droit interne, des restrictions destinées à contrôler l'exploitation non réglementée de données à caractère personnel contenues dans des fichiers publics à des fins de marketing. En ce qui concerne l'annuaire téléphonique, les sauvegardes mentionnées ci-dessus, permettant à l'abonné de ne pas figurer dans l'annuaire téléphonique, de ne pas recevoir de matériel publicitaire ou promotionnel ou de refuser que ses données soient communiquées à des tierces personnes à des fins de marketing, constituent aux yeux des rédacteurs de la recommandation des restrictions appropriées.

89. Il conviendrait également de se référer à la Recommandation no R (91) 10 sur la communication à des tierces personnes de données à caractère personnel détenues par des organismes publics, qui prévoit aussi certains critères qui devraient être respectés par les sociétés de marketing lorsqu'elles cherchent à exploiter des données à caractère personnel contenues dans des fichiers publics. Bien que le texte soit pertinent pour les activités d'exploitants du réseau public, les principes de cette recommandation peuvent être également utilisés par des exploitants privés en vue de déterminer les conditions dans lesquelles les listes d'abonnés peuvent être mises à la disposition des sociétés de marketing ou de vente par correspondance et exploitées par celles-ci.

90. Alors que les principes 4.1 et 4.3 concernent la communication des données à caractère personnel en général, le principe 7.8 exige que le droit interne établisse des garanties appropriées et détermine les conditions selon lesquelles les données à caractère personnel des abonnés peuvent être utilisées par les exploitants de réseau, par les fournisseurs de services ou par des tiers à des fins de marketing direct.

91. A l'instar de la Recommandation no R (85) 20, la présente recommandation souligne également l'utilité des codes d'autoréglementation comme moyen d'assurer l'environnement juridique et social approprié dans le domaine du télémarketing. Gardant cela à l'esprit, le

principe 7.9 encourage le secteur concerné à élaborer ses propres codes de conduite en vue d'assurer que le télémarketing ne provoque ni gêne ni harcèlement des abonnés. Le principe 7.9 indique un nombre de lignes directrices qui devraient être incorporées dans les codes de conduite. Plutôt que d'insérer dans l'annexe un principe sur l'interdiction d'adresser des messages publicitaires directement à des mineurs, les rédacteurs de la recommandation sont convenus que des codes de conduite devraient décourager cette pratique.

92. Bien que le texte souligne l'autoréglementation, il convient de garder à l'esprit que des codes de déontologie ou de conduite dans le secteur du télémarketing devraient être élaborés en conformité avec le droit interne, par exemple celui d'une législation sur la protection des données. Afin que ces codes deviennent effectifs et contraignants pour le secteur du télémarketing, ils devraient alors être approuvés par une autorité supérieure, par exemple l'autorité s'occupant de la mise en œuvre d'une législation sur la protection des données. Ces références à une législation sur la protection des données n'excluent pas la possibilité qu'une législation sur la protection des consommateurs puisse aborder les problèmes soulevés par le télémarketing, permettant ainsi l'autoréglementation dans le cadre d'une législation destinée à protéger les consommateurs.

93. Le principe 7.10 oblige les sociétés impliquées dans le télémarketing - et il est admis qu'y sont inclus le démarchage par téléphone, par fax, par courrier électronique ou tout autre moyen de télécommunication permettant la transmission de messages - à respecter le vœu des abonnés ne souhaitant pas recevoir de messages publicitaires. En conséquence, ces abonnés, dont les noms figurent sur des listes oranges ou sur des listes rouges, ou qui ont choisi par tout autre moyen de ne pas recevoir de messages publicitaires, ne devraient pas être contactés par des sociétés de télémarketing. Le principe 7.10 encourage, à cette fin, la tenue d'une liste "orange" de ces abonnés.

94. Les considérations indiquées ci-dessus concernant le télémarketing s'appliquent aux exploitants de réseau et aux fournisseurs de services ainsi qu'à tout autre organisme qui met sur le marché des moyens de télécommunication.

95. Une attention particulière est accordée aux problèmes soulevés par les appels automatiques, y compris par fax. Ces automates d'appel permettent d'envoyer au hasard des messages préenregistrés. Ils exploitent des listes de numéros qui sont composés sans interruption jusqu'à ce que l'abonné décroche. Le principe 7.11 indique très clairement que ce genre d'appels transmettant des messages préenregistrés de nature commerciale ne doivent être envoyés qu'aux abonnés ayant donné leur consentement à ce type de service (opting in: choix de participer). Ce genre d'appel peut être utilisé à d'autres fins que pour le marketing, par exemple pour informer les abonnés des résultats sportifs ou du cours de la Bourse. Dans ces cas, l'abonné paie généralement ce service et y a donc consenti.

96. Le texte passe sous silence la question de l'utilisation de messages préenregistrés pour avertir d'une urgence locale les abonnés vivant dans un quartier donné. Ils peuvent être utilisés pour informer la population globale d'urgences au niveau national. Cette pratique est acceptable. Il peut se produire également qu'un abonné soit contacté par l'exploitant de réseau pour le prévenir par message préenregistré que sa ligne téléphonique va être coupée prochainement pour non-paiement de sa facture téléphonique. L'abonné devrait consentir à ce genre de message préenregistré au moment de la signature de son contrat initial avec l'exploitant de réseau. Sinon, la transmission de message peut constituer à la fois une intrusion et une gêne pour l'abonné. Il peut aussi arriver que l'exploitant de réseau envoie des messages préenregistrés aux abonnés lors de l'arrivée d'un télégramme les concernant en leur demandant de le retirer à un bureau de poste déterminé. Cette pratique peut aussi s'avérer acceptable,

mais les abonnés devraient être informés lors de la signature de leur contrat avec l'exploitant de réseau que des messages de ce type peuvent leur être envoyés de façon préenregistrée.

97. Les situations dans lesquelles des messages préenregistrés pourraient être envoyés devraient être aussi limitées que possible.

c. Facturation détaillée

98. La mise à disposition de factures détaillées envoyées aux abonnés énumérant les appels effectués pendant une certaine période, les numéros appelés, le temps passé au téléphone, etc., présente des avantages énormes pour les consommateurs. Cela permet aux abonnés de vérifier l'exactitude de la facture qui leur a été envoyée par l'exploitant de réseau et de contester la facture s'ils estiment qu'elle a été incorrectement calculée. Il n'est pas étonnant que dans certains pays les consommateurs aient effectué des pressions vigoureuses pour l'obtention de factures détaillées.

99. Néanmoins, des problèmes urgents de protection des données sont soulevés par la mise à disposition de factures détaillées aux abonnés, ainsi que par la conservation, par l'exploitant du réseau, des données de service sur lesquelles la facture est fondée. En premier lieu, la facture détaillée envoyée à l'abonné lui permet d'examiner le comportement au téléphone des autres personnes vivant à son domicile et qui utilisent son téléphone. En particulier, elle permet à l'abonné principal d'identifier les correspondants des co-utilisateurs. En second lieu, le fait que les données de service soient enregistrées par l'exploitant de réseau crée le risque qu'elles puissent être utilisées à d'autres fins que de facturation. On peut atténuer ce risque en garantissant que cette facture ne soit pas conservée pendant une longue période par l'exploitant de réseau. Des solutions possibles à ces problèmes ont été avancées aux principes 7.12 et 7.13.

100. Confrontés à un conflit éventuel d'intérêts, les rédacteurs de la recommandation se sont efforcés de trouver un compromis acceptable. Le principe 7.12 établit la disposition selon laquelle une facture détaillée ne doit être envoyée à un abonné qu'à sa demande. En outre, lorsque d'autres utilisateurs se servent du téléphone de l'abonné - par exemple d'autres membres adultes de sa famille - il faudrait éviter d'entraver leur liberté d'utilisation du téléphone, résultant de la mise à disposition à l'abonné d'une facture détaillée établissant leurs opérations téléphoniques. Bien que l'on puisse argumenter en disant que les co-utilisateurs se servent du téléphone de l'abonné à leurs risques, l'abonné devrait au moins informer les co-utilisateurs du fait qu'il reçoit des factures détaillées régulièrement, et que celles-ci révéleront des informations concernant leur utilisation de son téléphone. Ils seront alors en mesure de modifier la façon de se servir du téléphone de l'abonné.

101. En ce qui concerne l'énumération des lignes appelées à partir du terminal de l'abonné, et comme évoqué plus haut, la vie privée des correspondants soulève un problème. Pour cette raison, les exploitants de réseau devraient fournir une facture détaillée rendant difficile ou impossible l'identification du titulaire de la ligne appelée. Quelques pays ont déjà développé ces pratiques. En se fondant sur ces pratiques, on pourrait supprimer les derniers chiffres de la ligne appelée.

102. Bien que l'anonymisation des numéros appelés devrait être encouragée, la facture complète peut en fait être enregistrée par l'exploitant du réseau. Si tel est le cas, les abonnés devraient alors être informés de cette pratique, conformément aux exigences liées à l'information citées plus haut au principe 3.2. Sauf dispositions légales exigeant une conservation plus longue de ces données, les données nécessaires à la facturation doivent être

effacées après paiement de la facture par l'abonné, tout en gardant à l'esprit que les données peuvent nécessiter un enregistrement pendant une période raisonnable, pour le cas où l'abonné aurait recours à des procédures juridiques afin de contester l'exactitude du montant dû. En tout cas, les données doivent être effacées à la clôture des procédures ou du règlement, ou lorsque la date limite d'une conservation légale est arrivée à échéance (principe 7.13).

d. Téléphonie interne

103. La recommandation ne se limite pas seulement à protéger les usagers des réseaux privés et publics de télécommunication ayant un statut officiel - par exemple parce qu'ils constituent des monopoles publics ou parce qu'ils bénéficient de concessions pour concourir avec ces monopoles. Dans les entreprises, on trouve normalement un système de téléphonie interne (Private Branch Exchange Systems), qui permet au personnel de communiquer par téléphone au sein même des organisations. Les systèmes de téléphonie interne existent également dans des établissements tels que des hôtels, où il y a une demande pour de telles installations téléphoniques. L'utilisation de ces systèmes donne lieu à l'enregistrement de données de service. Ainsi, les titulaires du réseau sont tenus d'enregistrer des données en vue de facturer à l'utilisateur le temps que durent les appels téléphoniques. Le calcul de la facture implique évidemment l'identification du bureau ou de la chambre d'hôtel à partir desquels l'appel est donné, le numéro appelé et la durée de l'appel.

Les rédacteurs de la recommandation sont convenus que les entreprises, hôtels, hôpitaux, restaurants, etc., qui mettent à la disposition de leurs employés ou clients un service interne de téléphone sont compris dans la définition des "fournisseurs de services" et, par conséquent, dans le champ d'application de la recommandation.

104. Le principe 7.14 de la recommandation tend à introduire une transparence dans la collecte et le traitement des données de service par les titulaires des systèmes de téléphonie interne. En règle générale, il devrait être porté à l'attention de l'utilisateur d'un téléphone (ou autre installation de télécommunication telle que fax ou courrier électronique) que l'utilisation du téléphone donne lieu à un enregistrement de données de service. Alors que le principe 7.15 se réfère à la Recommandation no R (89) 2 sur la protection des données à caractère personnel utilisées à des fins d'emploi, le principe 7.14 recommande simplement que, en dehors du contexte de l'emploi, "des moyens appropriés" soient trouvés pour informer les utilisateurs que des données sont enregistrées lorsqu'ils utilisent le téléphone. Ces "moyens appropriés" pourraient être concrétisés par l'apposition d'étiquettes sur les terminaux téléphoniques dans les hôtels, ou par la mise à disposition de brochures d'information près des téléphones dans les chambres d'hôtels. Les données de service devraient être effacées immédiatement après paiement de la facture par l'utilisateur.

105. Les rédacteurs de la recommandation ont reconnu que ce n'est pas toujours l'utilisateur qui paie la facture. Celle-ci peut être adressée à une autre personne - par exemple un employeur - pour paiement. En tout cas, le principe 7.12 s'applique aussi aux systèmes de téléphonie interne: en principe, la facture fournie par un exploitant de téléphonie interne devrait être présentée et transmise à une tierce personne de manière bienveillante et confidentielle. En particulier, la facture ne devrait contenir que le montant dû sans indiquer la nature des appels effectués.

106. Le principe 7.15 consacre une attention particulière à l'introduction et à l'utilisation d'un autocommutateur téléphonique sur les lieux de travail, et est fondé sur la Recommandation no R (89) 2. Cette recommandation s'inspire de la nécessité d'assurer que la collecte et l'enregistrement des données de service soient effectués licitement et loyalement, et que les

données ne soient pas utilisées à des fins telles que la surveillance du temps passé au téléphone par les employés dans leurs bureaux, en vue de tirer des conclusions sur des questions portant sur leur productivité ou leur comportement au travail.

e. Identification de la ligne d'appel

107. La numérisation des réseaux a rendu possible cette nouvelle caractéristique technique dans la téléphonie vocale. A l'aide d'un dispositif visuel sur le terminal d'un abonné, il est maintenant possible d'identifier la source des appels entrants, en d'autres termes d'identifier la partie appelante. Plusieurs pays d'Europe ont déjà introduit cette caractéristique technique. D'autres pays envisagent d'offrir aux abonnés au RNIS la possibilité d'identifier les numéros de téléphone des appelants encore reliés au réseau analogique.

108. Cette nouvelle caractéristique technique entraîne de nombreux avantages pour les abonnés. Tout d'abord, elle leur permet d'effectuer un contrôle lorsque le téléphone sonne. Avec la visualisation du numéro entrant avant même que la communication ne soit établie, l'abonné est en mesure de décider si oui ou non il désire parler à la partie appelante. Ensuite, la nouvelle caractéristique technique est un outil utile pour lutter contre les appels abusifs ou malveillants, étant donné que les responsables de ces appels ne pourront plus dissimuler longtemps leur identité (à condition bien entendu qu'ils téléphonent à partir d'un terminal relié au réseau RNIS). Enfin, la visualisation du numéro entrant sur le terminal de la partie appelée présente des avantages évidents pour les services d'urgence tels que la police, les ambulances et les sapeurs-pompiers. En bref, elle facilite à ces services la localisation des appelants en détresse, qui ne sont pas toujours en mesure de communiquer clairement leur emplacement et leur situation difficile.

109. D'autre part, les avantages perçus indiqués au paragraphe précédent méritent d'être évalués à la lumière d'un certain nombre de problèmes de vie privée qui ont été identifiés par la communauté de la protection des données. Tout d'abord, la caractéristique technique peut éventuellement saper l'anonymat garanti par les listes rouges. Ensuite, l'identification de la ligne d'appel constitue un obstacle à la liberté de communication des individus qui contactent des services d'assistance tels que les alcooliques anonymes, les centres d'accueil ou les Samaritains. Les individus sont encouragés à contacter cette catégorie de services sur la base du respect de leur anonymat. Les abonnés seront évidemment découragés de téléphoner à ces services d'assistance s'ils savent que leur numéro de téléphone sera révélé. Un problème similaire se pose au regard des lignes confidentielles établies pour des besoins d'enquête de police. Enfin, la cession d'un numéro de téléphone à une entreprise commerciale ou de démarchage résultant d'une enquête téléphonique concernant un produit ou un service particulier peut occasionner des appels non souhaités de nature commerciale ou de démarchage.

110. C'est dans le contexte de ces problèmes que le principe 7.16 exige que les abonnés soient informés du fait qu'il est possible d'identifier la ligne d'appel. De plus, les rédacteurs de la recommandation sont convenus de l'utilité pour la partie appelante de supprimer l'affichage de son numéro de téléphone sur le terminal de la partie appelée. Cela pourrait être réalisé, par exemple, en incorporant dans les terminaux téléphoniques un moyen technique simple tel qu'un bouton-poussoir qui, lorsqu'il est actionné, permettrait à l'appelant de garder l'anonymat. La recommandation n'exige pas que la partie appelante puisse annuler soit définitivement l'affichage de son numéro (et conserver ainsi les avantages des listes rouges) soit ponctuellement en fonction des appels, ce qui constituerait une alternative possible mais non obligatoire de la suppression permanente de l'affichage du numéro.

111. Bien qu'il soit généralement admis que les abonnés appelants, qui ont un intérêt légitime à préserver leur anonymat, devraient avoir la possibilité d'éviter l'affichage de leurs numéros de téléphone, les rédacteurs de la recommandation sont convenus que les coûts pour fournir également un tel service aux abonnés appelés l'emportent, pour le moment, sur leurs intérêts.

112. Les rédacteurs de la recommandation sont convenus également que, en vue des discussions en cours dans certains Etats, il serait prématuré d'exiger que la partie appelante ne supporte pas de coûts supplémentaires liés à la suppression de l'identification de la ligne d'appel.

113. Dans certaines circonstances, il peut être nécessaire d'outrepasser la décision de la partie appelante visant à presser le bouton pour maintenir son anonymat. Par exemple, les service d'urgence (police, pompiers, etc.) devraient toujours avoir la possibilité d'accéder à la visualisation du numéro de l'appelant. De plus, un abonné harassé par des appels malveillants ou abusifs, de même qu'un service d'urgence dérangé par des canulars, peut charger l'exploitant du réseau d'annuler les instructions qui lui ont été données par la partie appelante. Cette décision ne doit pas être prise facilement, et c'est pourquoi le principe 7.17 prévoit que le droit interne devrait déterminer les conditions et garanties qui doivent exister avant que cette dérogation n'ait lieu.

f. Transfert d'appel

114. Le transfert d'appel (ou "renvoi temporaire") permet à un abonné de renvoyer ses appels entrants sur le terminal d'un tiers abonné. Ce service ne dépend pas de la numérisation du réseau, étant donné qu'il a toujours été disponible dans le système analogique. Les principes 7.18 et 7.19 de la recommandation cherchent à établir quelques lignes directrices pour assurer la commodité des tiers abonnés vers lesquels les appels entrants sont transférés par les abonnés appelés.

115. En premier lieu, le tiers abonné devrait être informé avant que l'abonné ne prenne la décision de transférer ses appels entrants sur le terminal du tiers abonné. Deuxièmement, en cas de désaccord, le tiers abonné devrait pouvoir obtenir de l'exploitant de réseau l'annulation du transfert d'appel.

En raison, d'une part, du fait que la recommandation n'est en principe pas adressée aux abonnés et, d'autre part, dans le souci de développer la responsabilité des abonnés eux-mêmes, les rédacteurs de la recommandation n'ont pas souhaité inclure de disposition visant à ce qu'un abonné devrait informer le tiers abonné de son intention de transférer ses appels entrants sur son terminal.

La recommandation prévoit, néanmoins, qu'en cas de désaccord, il devrait être possible d'annuler le transfert d'appel (principe 7.18).

116. La recommandation ne concerne pas la situation dans laquelle les parties appelantes ne sont pas au courant du fait qu'un appel est renvoyé vers le terminal d'un tiers abonné. Bien qu'il puisse être justifié de permettre à la partie appelante d'être informée de cette situation, les rédacteurs de la recommandation ont aussi noté les risques que cela présente pour la sécurité. On a pensé qu'il n'était pas souhaitable d'informer les parties appelantes du fait que la partie appelée n'était pas chez elle.

117. Le principe 7.19 traite de la situation dans laquelle une bande ou des écoutes ont été placées sur le téléphone d'un abonné conformément aux dispositions du principe 2.4, et où

l'abonné a transféré ses appels entrants sur le terminal d'un tiers abonné. Il y a un risque technique potentiel pour que le tiers abonné et son cercle de correspondants se retrouvent dans le filet. C'est pourquoi le principe 7.19 préconise que, pour autant que c'est techniquement possible, seuls les appels entrants de la personne suspecte devraient faire l'objet de mesures de surveillance, à l'exclusion des appels entrants destinés au tiers abonné.

118. Comme au principe 2.4 (voir le paragraphe 34 ci-dessus), la référence, dans le principe 7.19, aux mesures de surveillance devrait être comprise comme s'appliquant à l'emploi des dispositifs ou d'autres moyens qui, de par leur nature, ont été désignés pour effectuer des ingérences dans les télécommunications, soit par interception soit par d'autres moyens.

g. Téléphonie mobile

119. La vitesse à laquelle le service des téléphones mobiles a été adopté par les abonnés, parfois inspirés par la mode, a conduit à négliger les problèmes sérieux soulevés par leur utilisation. La recommandation a identifié deux questions qui devraient être traitées:

i. la vulnérabilité des téléphones mobiles en tant que moyen de communication;

ii. leur capacité à engendrer l'enregistrement de données de service avec ingérence potentielle dans la vie privée de l'usager.

120. En traitant de la question de vulnérabilité, la recommandation note que l'utilisation des services de téléphones mobiles manque de moyens sûrs pour maintenir la confidentialité des communications. L'interception des conversations est facilitée. Cela pose un problème pour les personnes qui utilisent des téléphones mobiles. Ayant cela à l'esprit, le principe 7.20 propose que les exploitants de réseaux devraient clairement informer leurs abonnés du caractère vulnérable de la transmission des messages par voie de téléphones mobiles. Bien que le principe 7.20 n'implique pas que l'exploitant du réseau fournisse un service de chiffrement en vue d'augmenter la sécurité de la transmission des messages, on pense, néanmoins, que des moyens devraient être mis au point pour offrir aux abonnés la possibilité de profiter de méthodes de chiffrement.

121. Comme au principe 2.2 (voir le paragraphe 27 ci-dessus), l'obligation des exploitants de réseau et fournisseurs de services de mettre au point, en vertu du principe 7.20, des moyens permettant aux abonnés au réseau de téléphones mobiles le chiffrement de leurs communications ou offrant des garanties équivalentes ne devrait pas être interprétée comme une interdiction pour les Etats membres de régler d'une façon ou d'une autre l'utilisation des algorithmes cryptographiques, afin de reproduire l'information d'origine dans un texte clair et compréhensible dans des cas où les télécommunications ont été interceptées sur ordre des autorités en vertu des règles en vigueur et en tenant compte des garanties en question.

Les moyens à mettre au point permettant le chiffrement ou offrant des garanties équivalentes devraient être tels qu'ils garantissent la possibilité d'effectuer une ingérence dans le contenu d'une communication conformément aux principes 2.3 et 2.4.

122. En ce qui concerne l'enregistrement des données de service, on devrait tenir compte du fait que le réseau de téléphones mobiles sera bientôt numérique, pour permettre aux abonnés de transmettre à partir de leurs téléphones de voiture des messages par fax, de la messagerie vocale, des images et des données. Comme pour la numérisation de tous les réseaux, la quantité de données de service enregistrées par les exploitants de réseaux de téléphones mobiles augmentera considérablement. Et comme pour tous les réseaux, il devient de plus en

plus important de définir avec précision les finalités pour lesquelles les données de service peuvent légitimement être détenues par l'exploitant du réseau qui offre des installations de téléphones mobiles. L'enregistrement devrait être limité aux finalités suivantes: connexion de l'abonné au réseau et traitement des données de service pour permettre l'envoi de la facture à l'abonné. Bien qu'il soit admis que la localisation de l'utilisateur doive être consignée quand il entre dans le système en vue de déterminer la zone dans laquelle il se trouve ainsi que sa localisation au moment où il donne des appels, le principe 7.21 cherche à obtenir que ces données ne soient pas utilisées pour établir un profil des déplacements de l'utilisateur ni pour déterminer l'identité de ses correspondants. Ces risques ont conduit les rédacteurs de la recommandation à suggérer que les données nécessaires à l'établissement de la facture reposent sur une large aire géographique plutôt que sur des détails précis de la localisation exacte de l'utilisateur lorsqu'il change de zone ou donne un appel. Le système de la tarification pourrait refléter cette suggestion.

Footnotes

1. Il est fait référence ci-dessous à "la Convention".

2. Les nouvelles technologies: un défi pour la protection de la vie privée?, Strasbourg, Conseil de l'Europe, 1989, ISBN 92-871-1616-4.