

PROTECTION DES DONNEES A CARACTERE PERSONNEL**Sommaire****I – Textes luxembourgeois**

- | | |
|--|-----|
| 1. Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel | 189 |
| 2. Projet de loi n° 5181 du 11 juillet 2003 relatif aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques et portant modification des articles 88-2 et 88-4 du Code d'instruction criminelle, et de la loi du 2 août 2002 relative à la protection de la personne à l'égard du traitement des données à caractère personnel | 211 |
| 3. Autres références | 229 |

II - Textes communautaires

- | | |
|--|-----|
| 1. Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données | 230 |
| 2. Directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques | 249 |
| 3. Autres références | 262 |

III - Textes internationaux

- | | |
|--|-----|
| 1. Convention du Conseil de l'Europe, du 28 janvier 1981, pour la protection des personnes à l'égard du traitement des données à caractère personnel dite «convention 108 du Conseil de l'Europe» | 263 |
| 2. Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, du 8 novembre 2001 concernant les autorités de contrôle et les flux transfrontières de données. | 269 |
| 3. Autres références | 271 |

I – Textes luxembourgeois

Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

(Mém. A - 91 du 13 août 2002, p.1836)

Chapitre 1^{er}. - Dispositions générales relatives à la protection de la personne à l'égard des traitements des données à caractère personnel

Art. 1^{er}. Objet

La présente loi protège les libertés et les droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel et fait respecter les intérêts légalement protégés des personnes morales.

Art. 2. Définitions

Aux fins de la présente loi, on entend par:

(a) «code de conduite»: contributions sectorielles élaborées en vue de la bonne application de la présente loi. Les codes de conduite sont élaborés à l'échelon national ou communautaire par les associations professionnelles et les autres organisations représentatives des responsables du traitement et sont facultativement soumis pour approbation à la Commission nationale ou au groupe de protection des personnes à l'égard du traitement des données à caractère personnel tel qu'institué par l'article 29 de la Directive 95/46/CE;

(b) «Commission nationale»: la Commission nationale pour la protection des données;

(c) «consentement de la personne concernée»: toute manifestation de volonté expresse, non équivoque, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal, judiciaire ou statutaire accepte que les données à caractère personnel fassent l'objet d'un traitement;

(d) «destinataire»: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données, qu'il s'agisse ou non d'un tiers; les autorités qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre de l'exécution d'une mission légale d'enquête ou de contrôle ne sont pas considérées comme des destinataires;

(e) «donnée à caractère personnel» (ci-après dénommée «donnée»): toute information de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image, concernant une personne identifiée ou identifiable («personne concernée»); une personne physique ou morale est réputée identifiable si elle peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique;

(f) «donnée relative à la santé»: toute information concernant l'état physique et mental d'une personne concernée, y compris les données génétiques;

(g) «donnée génétique»: toute donnée concernant les caractères héréditaires d'un individu ou d'un groupe d'individus apparentés;

(h) «fichier de données à caractère personnel» (ci-après dénommé «fichier»): tout ensemble structuré de données accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique;

(i) «instance médicale»: tout praticien de la santé et toute personne soumise à la même obligation de secret professionnel, ainsi que tout établissement hospitalier visé par la loi du 28 août 1998 sur les établissements hospitaliers, effectuant un traitement de données nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion de services de santé;

(j) «interconnexion»: toute forme de traitement qui consiste en la corrélation de données traitées pour une finalité avec des données traitées pour des finalités identiques ou liées par un ou d'autres responsables du traitement;

(k) «ministre»: le ministre ayant dans ses attributions la protection des données;

(l) «organisme de sécurité sociale»: tout organisme de droit public ou privé qui assure des prestations, obligatoires ou facultatives, relatives à la maladie, la maternité, la vieillesse, les accidents corporels, l'invalidité, la dépendance, le décès, le chômage, ainsi que des prestations familiales ou d'aides sociales;

(m) «pays tiers»: Etat non membre de l'Union européenne;

(n) «personne concernée»: toute personne physique ou morale, publique ou privée ou groupement de fait, qui fait l'objet d'un traitement de données à caractère personnel;

(o) «responsable du traitement»: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel. Lorsque les finalités et les moyens du traitement sont déterminés par ou en vertu des dispositions légales, le responsable du traitement est déterminé par ou en vertu des critères spécifiques conformément aux dispositions légales;

(p) «sous-traitant»: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données pour le compte du responsable du traitement;

(q) «surveillance»: toute activité faisant appel à des moyens techniques en vue de détecter, d'observer, de copier ou d'enregistrer les mouvements, images, paroles, écrits, ou l'état d'un objet ou d'une personne fixe ou mobile;

(r) «tiers»: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placés sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilités à traiter les données. Dans le secteur public, on entend par tiers un ministère, une administration, un établissement public, une commune ou un service public autre que le responsable du traitement ou son sous-traitant;

(s) «traitement de données à caractère personnel» (ci-après dénommé «traitement»): toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés, et appliquées à des données, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

Art. 3.- Champ d'application

(1) La présente loi s'applique au traitement automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données contenues ou appelées à figurer dans un fichier.

(2) Sont soumis à la présente loi:

(a) le traitement mis en œuvre par un responsable du traitement soumis au droit luxembourgeois;

(b) le traitement mis en œuvre par un responsable du traitement qui, sans être établi sur le territoire luxembourgeois ou sur celui d'un autre Etat membre de l'Union européenne, recourt à des moyens de traitement situés sur le territoire luxembourgeois, à l'exclusion des moyens qui ne sont utilisés qu'à des fins de transit sur ce territoire ou sur celui d'un autre Etat membre de l'Union européenne.

Pour le traitement mentionné à l'article 3, paragraphe (2) lettre (b), le responsable du traitement désigne par une déclaration écrite à la Commission nationale un représentant établi sur le territoire luxembourgeois qui se substitue au responsable du traitement dans l'accomplissement de ses obligations prévues par la présente loi sans que ce dernier ne soit déchargé de sa propre responsabilité.

(3) La présente loi s'applique au traitement de données concernant la sécurité publique, la défense, la recherche et la poursuite d'infractions pénales ou la sûreté de l'Etat, même liées à un intérêt économique ou financier important de l'Etat, sans préjudice des dispositions spécifiques de droit national ou international régissant ces domaines.

(4) La présente loi s'applique à toute forme de captage, de traitement et de diffusion de sons et images qui permettent d'identifier des personnes physiques ou morales.

(5) La présente loi ne s'applique pas:

- au traitement mis en œuvre par une personne physique dans le cadre exclusif de ses activités personnelles ou domestiques,
- au traitement de données concernant une personne morale et dont la publication est prescrite par une loi ou un règlement.

Chapitre II. - Conditions de licéité du traitement

Art. 4. Qualité des données

(1) Le responsable du traitement doit s'assurer que les données qu'il traite le sont loyalement et licitement, et notamment que ces données sont:

- (a) collectées pour des finalités déterminées, explicites et légitimes, et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités;
- (b) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement;
- (c) exactes et, si nécessaire, mises à jour; toute mesure raisonnable doit être prise pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées;
- (d) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées et traitées sans préjudice du paragraphe (2) ci-après.

(2) Les données traitées à des finalités déterminées peuvent être traitées ultérieurement à des fins historiques, statistiques ou scientifiques et sont soumises aux conditions prévues par le régime d'autorisation préalable de la Commission nationale tel que prévu à l'article 14.

(3) Quiconque effectue un traitement en violation des dispositions du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 5. Légitimité du traitement

(1) Le traitement de données ne peut être effectué que si:

- (a) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis, ou si
- (b) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées, ou si
- (c) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci, ou si
- (d) le traitement est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1^{er}, ou si
- (e) le traitement est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée, ou si
- (f) la personne concernée a donné son consentement.

(2) Quiconque effectue un traitement en violation des dispositions du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 6. Traitement de catégories particulières de données

(1) Les traitements qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les traitements de données relatives à la santé et à la vie sexuelle, y compris le traitement des données génétiques sont interdits.

(2) Le paragraphe (1) ne s'applique pas lorsque:

- (a) la personne concernée a donné son consentement à un tel traitement, sauf indisponibilité du corps humain et sauf le cas interdit par la loi, ou lorsque
- (b) le traitement est nécessaire aux fins de respecter les obligations et les droits spécifiques du responsable du traitement notamment en matière de droit du travail dans la mesure où il est autorisé par la loi, ou lorsque

- (c) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement, ou lorsque
- (d) le traitement est mis en œuvre, avec le consentement de la personne concernée par une fondation, une association ou tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale, dans le cadre de leurs activités légitimes, à condition que le traitement se rapporte aux données nécessaires des seuls membres de cet organisme ou aux personnes entretenant avec lui des contacts réguliers liés à sa finalité et que les données ne soient pas communiquées à des tiers sans le consentement des personnes concernées, ou lorsque
- (e) le traitement porte sur des données manifestement rendues publiques par la personne concernée, ou lorsque
- (f) le traitement mis en œuvre conformément aux règles de procédures judiciaires applicables en matière civile est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice s'il est mis en œuvre à cette fin exclusive, ou lorsque
- (g) le traitement s'avère nécessaire pour un motif d'intérêt public notamment à des fins historiques, statistiques ou scientifiques sans préjudice de l'application de l'article 7 ci-après et que ce traitement est mis en œuvre conformément au régime d'autorisation préalable de la Commission nationale tel que prévu à l'article 14, ou lorsque
- (h) le traitement est mis en œuvre par voie de règlement grand-ducal tel que prévu à l'article 17.

(3) L'article 6 paragraphe (1) ne s'applique pas lors d'une procédure judiciaire ou d'une enquête pénale. Toutefois les données génétiques ne peuvent être traitées que pour vérifier l'existence d'un lien génétique dans le cadre de l'administration de la preuve en justice, pour l'identification d'une personne, la prévention ou la répression d'une infraction pénale déterminée.

(4) Par dérogation à l'article 6, paragraphe (1), les données génétiques ne peuvent faire l'objet d'un traitement que:

- (a) dans les cas visés par les articles 6, paragraphe (2) lettres (c), (f), (g), (h), 6 paragraphe (3) et 7 de la présente loi, ou lorsque
- (b) la personne concernée a donné son consentement et si le traitement est effectué dans les seuls domaines de la santé ou de la recherche scientifique sauf indisponibilité du corps humain et dans le cas où la loi prévoit que l'interdiction visée au paragraphe (1) ne peut être levée par le consentement de la personne concernée.

(5) Quiconque effectue un traitement ou opère une communication à un tiers en violation des dispositions du paragraphe (1) qui précède est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement ou de la communication contraires aux dispositions du paragraphe (1) du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 7. Traitement de catégories particulières de données par les services de la santé

(1) Lorsque le traitement de données tel que défini à l'article 6 paragraphe (1) de la présente loi est nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion de services de santé, de la recherche scientifique dans le domaine de la biologie et de la médecine, le traitement de ces données peut être mis en œuvre par des instances médicales, ainsi que lorsque le responsable du traitement est soumis au secret professionnel, par les organismes de sécurité sociale et les administrations qui gèrent ces données en exécution de leurs missions légales et réglementaires, par les entreprises d'assurance, les sociétés gérant les fonds de pension, la Caisse médico-chirurgicale mutualiste et par celles des personnes physiques ou morales bénéficiant d'un agrément dans le domaine médico-social ou thérapeutique en vertu de la loi du 8 septembre 1998 réglant les relations entre l'Etat et les organismes œuvrant dans les domaines social, familial et thérapeutique, désignées par règlement grand-ducal. Le recours à un sous-traitant est possible dans les conditions prévues à l'article 21.

(2) Le traitement visé ci-dessus fait l'objet d'une autorisation préalable de la Commission nationale.

(3) Par dérogation au paragraphe (2) qui précède sont soumis à notification:

- le traitement mis en œuvre conformément à l'article 36 de la loi du 28 août 1998 sur les établissements hospitaliers;
- le traitement mis en œuvre par un médecin et concernant ses patients.

(4) Sous réserve que leur traitement soit en lui-même licite au regard des articles 6 et 7, les données y visées peuvent être communiquées à des tiers ou utilisées à des fins de recherche, d'après les modalités et suivant les conditions à déterminer par règlement grand-ducal.

(5) Quiconque effectue un traitement ou opère une communication à un tiers en violation des dispositions du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement ou de la communication contrairement aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 8. Traitement de données judiciaires

(1) Le traitement des données dans le cadre d'enquêtes pénales et de procédures judiciaires est opéré dans le respect des dispositions du Code d'instruction criminelle, du Code de procédure civile, de la loi portant règlement de procédure devant les juridictions administratives ou d'autres lois.

(2) Le traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peut être mis en œuvre qu'en exécution d'une disposition légale.

(3) Il ne peut être tenu de recueil exhaustif des condamnations pénales que sous le contrôle de l'autorité publique compétente en la matière.

(4) Quiconque, agissant à titre privé, effectue un traitement en violation des dispositions du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement.

La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 9. Traitement réalisé dans le cadre de la liberté d'expression

(1) Sans préjudice des dispositions prévues dans la législation sur la liberté dans les moyens de communication de masse et dans la mesure où les dérogations ci-après s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression, le traitement mis en œuvre aux seules fins de journalisme ou d'expression artistique ou littéraire n'est pas soumis:

- (a) - à la prohibition de traiter les catégories particulières de données telle que prévue à l'article 6, paragraphe (1);
 - aux limitations concernant le traitement de données judiciaires prévues à l'article 8; lorsque le traitement se rapporte à des données rendues manifestement publiques par la personne concernée ou à des données qui sont en relation étroite avec le caractère public de la personne concernée ou du fait dans lequel elle est impliquée;
- (b) à la condition de protection adéquate exigée s'agissant des traitements de données faisant l'objet d'un transfert vers un pays tiers telle que prévue à l'article 18, paragraphe (1);
- (c) à l'obligation d'information de l'article 26, paragraphe (1), lorsque son application compromettrait la collecte des données auprès de la personne concernée;
- (d) à l'obligation d'information de l'article 26, paragraphe (2), lorsque son application compromettrait soit la collecte des données, soit une publication en projet, soit la mise à disposition du public, de quelque manière que ce soit de ces données ou fournirait des indications permettant d'identifier les sources d'information;
- (e) au droit d'accès de la personne concernée qui peut être différé ou limité conformément à l'article 28, paragraphe (4) et à l'article 29.

(2) Lors de la notification d'un traitement effectué à des fins de journalisme ou d'expression artistique ou littéraire, la notification ne renseigne que sur le(s) nom(s) et adresse(s) du responsable du traitement ou de son représentant.

Art. 10. Traitement à des fins de surveillance

(1) Le traitement à des fins de surveillance ne peut être effectué que:

- (a) si la personne concernée a donné son consentement, ou
- (b) aux abords ou dans tout lieu accessible ou non au public autres que les locaux d'habitation, notamment dans les parkings couverts, les gares, aéroports et les moyens de transports publics, pourvu que le lieu en question présente de par sa nature, sa situation, sa configuration ou sa fréquentation un risque rendant le traitement nécessaire à la sécurité des usagers ainsi qu'à la prévention des accidents, ou

(c) aux lieux d'accès privé dont la personne physique ou morale y domiciliée est le responsable du traitement.

(2) Les personnes concernées sont informées par des moyens appropriés tels que des panneaux de signalisation, des circulaires et/ou des envois recommandés par voie postale ou électronique de la mise en œuvre des traitements visés au paragraphe (1), lettres (b) et (c). A la demande de la personne concernée, le responsable du traitement fournit à celle-ci les informations prévues à l'article 26, paragraphe (2).

(3) Les données collectées à des fins de surveillance ne sont communiquées que:

(a) si la personne concernée a donné son consentement sauf le cas interdit par la loi, ou

(b) aux autorités publiques dans le cadre de l'article 17, paragraphe (1), ou

(c) aux autorités judiciaires compétentes pour constater ou poursuivre une infraction pénale et aux autorités judiciaires devant lesquelles un droit en justice est exercé ou défendu.

(4) Quiconque effectue un traitement en violation des dispositions du paragraphe (1) qui précède est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du paragraphe (1) du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 11. Traitement à des fins de surveillance sur le lieu du travail

(1) Le traitement à des fins de surveillance sur le lieu de travail peut être mis en œuvre, conformément à l'article 14, par l'employeur s'il en est le responsable. Un tel traitement n'est possible que s'il est nécessaire:

(a) pour les besoins de sécurité et de santé des travailleurs, ou

(b) pour les besoins de protection des biens de l'entreprise, ou

(c) pour le contrôle du processus de production portant uniquement sur les machines, ou

(d) pour le contrôle temporaire de production ou des prestations du travailleur, lorsqu'une telle mesure est le seul moyen pour déterminer la rémunération exacte, ou

(e) dans le cadre d'une organisation de travail selon l'horaire mobile conformément à la loi.

Dans les cas visés aux lettres (a), (d) et (e), le comité mixte d'entreprise, le cas échéant institué, a un pouvoir de décision tel que défini à l'article 7, paragraphes (1) et (2), de la loi modifiée du 6 mai 1974 instituant des comités mixtes dans les entreprises du secteur privé et organisant la représentation des salariés dans les sociétés anonymes.

Le consentement de la personne concernée ne rend pas légitime le traitement mis en œuvre par l'employeur.

(2) Sans préjudice du droit à l'information de la personne concernée sont informés préalablement par l'employeur:

- la personne concernée, ainsi que

- pour les personnes tombant sous l'empire de la législation sur le contrat de droit privé: le comité mixte ou à défaut la délégation du personnel ou à défaut encore l'Inspection du travail et des mines;

- pour les personnes tombant sous l'empire d'un régime statutaire: les organismes de représentation du personnel tels que prévus par les lois et règlements afférents.

(3) Quiconque effectue un traitement en violation des dispositions du présent article est puni d'une peine d'emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement.

La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Chapitre III. - Formalités préalables à la mise en œuvre des traitements et publicités des traitements

Art. 12. Notification préalable à la Commission nationale

(1) (a) A l'exception de ceux qui relèvent des dispositions prévues aux articles 8, 14 et 17, les traitements de données font l'objet d'une notification préalable par le responsable du traitement auprès de la Commission nationale.

(b) Les traitements relevant d'un même responsable du traitement et ayant des finalités identiques ou liées entre elles peuvent faire l'objet d'une notification unique. Dans ce cas les informations

requis en application de l'article 13 ne sont fournies pour chacun des traitements que dans la mesure où elles lui sont propres.

(2) Pour les traitements des données dont la mise en œuvre n'est pas susceptible de porter atteinte aux libertés et droits fondamentaux, et notamment à la vie privée, des personnes concernées, la Commission nationale établit et publie des directives en vue d'une notification simplifiée.

Ces directives précisent:

- a) la ou les finalités du traitement faisant l'objet d'une notification simplifiée;
- b) la ou les catégories de données traitées;
- c) la ou les catégories de personnes concernées;
- d) les destinataires ou catégories de destinataires auxquels les données sont communiquées;
- e) la durée de conservation.

Les traitements qui correspondent à ces directives font l'objet d'une notification simplifiée de conformité envoyée à la Commission nationale le cas échéant par voie électronique.

(3) Est exempté de l'obligation de notification:

- (a) le responsable du traitement qui désigne un chargé de la protection des données tenu notamment d'assurer, de manière indépendante, l'application des dispositions légales en la matière et d'établir et de continuer à la Commission nationale un registre des traitements effectués par le responsable du traitement conformément aux dispositions relatives à la publicité des traitements telles que prévues à l'article 15;
- (b) le traitement ayant pour seul objet la tenue d'un registre qui en vertu d'une disposition légale est destiné à l'information du public et qui est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime;
- (c) le traitement mis en œuvre conformément aux règles de procédures judiciaires en matière civile et nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice.

(4) Quiconque ne se soumet pas à l'obligation de notification ou fournit des informations incomplètes ou inexacts est puni d'une amende de 251 à 125.000 euros. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 13. Contenu et forme de la notification

(1) La notification comprend au moins les informations suivantes:

- (a) le nom et l'adresse du responsable du traitement, et le cas échéant de son représentant et du sous-traitant;
- (b) la condition de légitimité du traitement;
- (c) la ou les finalité(s) du traitement;
- (d) la description de la ou des catégories de personnes concernées et des données ou des catégories de données s'y rapportant;
- (e) les destinataires ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées;
- (f) les pays tiers à destination desquels des transferts de données sont envisagés;
- (g) une description générale permettant d'apprécier de façon préliminaire le caractère approprié des mesures prises pour assurer la sécurité du traitement en application des articles 22 et 23;
- (h) la durée de conservation des données.

(2) Toute modification affectant les informations visées au paragraphe (1) doit être notifiée à la Commission nationale préalablement à la mise en œuvre du traitement.

(3) La notification se fait auprès de la Commission nationale moyennant support papier ou informatique suivant un schéma à établir par elle. Il est accusé réception de la notification.

(4) Un règlement grand-ducal fixera le montant et les modalités de paiement d'une redevance à percevoir lors de toute notification et de toute modification de notification.

Art. 14. Autorisation préalable de la Commission nationale

(1) Sont soumis à l'autorisation préalable de la Commission nationale:

- (a) les traitements prévus à l'article 6, paragraphe (2) lettres (a), (b), (e), (g), et paragraphe (4) lettre (b), à l'article 7, paragraphe (1), et aux articles 10 et 11 de la présente loi;
- (b) les traitements de données à des fins historiques, statistiques ou scientifiques visés à l'article 4, paragraphe (2).

La Commission nationale vérifie en particulier si ces traitements ne peuvent être réalisés sur base de données rendues anonymes;

- (c) l'interconnexion de données visée à l'article 16;
- (d) le traitement concernant le crédit et la solvabilité des personnes concernées;
- (e) l'utilisation de données à des fins autres que celles pour lesquelles elles ont été collectées. Un tel traitement ne peut être effectué que moyennant consentement préalable de la personne concernée.

(2) La demande d'autorisation comprend les informations suivantes:

- (a) le nom et l'adresse du responsable du traitement ou de son représentant et le cas échéant du sous-traitant;
- (b) la condition de légitimité du traitement;
- (c) la ou les finalités du traitement;
- (d) l'origine des données;
- (e) la description détaillée des données ou catégories de données ainsi que des traitements envisagés;
- (f) la description de la ou des catégories de personnes concernées;
- (g) les destinataires ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées;
- (h) les pays tiers à destination desquels des transferts de données sont envisagés;
- (i) une description détaillée permettant d'apprécier le respect des mesures de sécurité prévues aux articles 22 et 23;
- (j) la durée de conservation des données.

(3) Les traitements qui ont une même finalité, qui portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires peuvent être autorisés par une décision unique de la Commission nationale. Dans ce cas le responsable de chaque traitement adresse à la Commission nationale un engagement formel de conformité de celui-ci à la description figurant dans l'autorisation.

(4) Quiconque effectue un traitement en violation des dispositions du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 15. Publicité des traitements

(1) La Commission nationale tient un registre public des traitements.

(2) Figurent dans ce registre:

- (a) les traitements notifiés à la Commission nationale en vertu de l'article 12, paragraphe (1);
- (b) les traitements autorisés par la Commission nationale en vertu de l'article 14, paragraphe (1); et
- (c) les traitements surveillés par le chargé de la protection des données et continués à la Commission nationale en vertu de l'article 12, paragraphe (3) (a).

(3) Le registre tenu par la Commission nationale contient sur chaque traitement les informations requises respectivement par l'article 13, paragraphe (1) et par l'article 14, paragraphe (2). Pour les traitements soumis à autorisation préalable, le registre renseigne en plus sur l'autorisation émise par la Commission nationale.

(4) Toute personne peut prendre connaissance, et ce gratuitement, des informations contenues dans le registre public qui est en ligne, à l'exception de celles prévues respectivement à l'article 13, paragraphe (1) lettre (g) et à l'article 14, paragraphe (2) lettre (i).

(5) Cependant la Commission nationale peut limiter cette publicité lorsqu'une telle mesure est nécessaire pour sauvegarder:

- (a) la sûreté de l'Etat,

- (b) la défense,
- (c) la sécurité publique,
- (d) la prévention, la recherche, la constatation et la poursuite d'infractions pénales y compris celles à la lutte contre le blanchiment, ou le déroulement de procédures judiciaires autres, au sens de l'article 8, paragraphe (1), et de l'article 17 de la présente loi,
- (e) un intérêt économique ou financier important de l'Etat ou de l'Union Européenne, y compris dans les domaines monétaire, budgétaire et fiscal,
- (f) la protection de la personne concernée ou des droits et libertés d'autrui,
- (g) la liberté d'expression,
- (h) une mission de contrôle, d'inspection ou de réglementation relevant, même à titre occasionnel, de l'exercice de l'autorité publique, dans les cas visés aux points (c), (d) et (e) et
- (i) le secret professionnel et le secret d'affaires de la personne concernée et du responsable du traitement.

(6) La Commission nationale publie un rapport annuel qui fait état des notifications et autorisations.

(7) Le présent article ne s'applique pas aux traitements ayant pour seul but la tenue d'un registre qui, en vertu d'une loi ou d'un règlement grand-ducal, est destiné à l'information du public et qui est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime.

Art. 16. Interconnexion de données

(1) L'interconnexion de données qui n'est pas expressément prévue par un texte légal doit faire l'objet d'une autorisation préalable de la Commission nationale sur demande conjointe présentée par les responsables des traitements en cause.

(2) L'interconnexion de données doit permettre d'atteindre des objectifs légaux ou statutaires présentant un intérêt légitime pour les responsables des traitements, ne pas entraîner de discrimination ou de réduction des droits, libertés et garanties pour les personnes concernées, être assortie de mesures de sécurité appropriées et tenir compte du type de données faisant l'objet de l'interconnexion.

(3) L'interconnexion n'est autorisée que dans le respect des finalités identiques ou liées de fichiers et du secret professionnel auquel les responsables du traitement sont le cas échéant astreints.

Art. 17. Autorisation par voie réglementaire

(1) Font l'objet d'un règlement grand-ducal:

- (a) les traitements d'ordre général nécessaires à la prévention, à la recherche et à la constatation des infractions pénales qui sont réservés, conformément à leurs missions légales et réglementaires respectives, aux organes du corps de la police grand-ducale, de l'Inspection générale de la police et de l'administration des douanes et accises.

Le règlement grand-ducal déterminera le responsable du traitement, la condition de légitimité du traitement, la ou les finalités du traitement, la ou les catégories de personnes concernées et les données ou les catégories de données s'y rapportant, l'origine de ces données, les tiers ou les catégories de tiers auxquels ces données peuvent être communiquées et les mesures à prendre pour assurer la sécurité du traitement en application de l'article 22 de la présente loi,

- (b) les traitements relatifs à la sûreté de l'Etat, à la défense et à la sécurité publique, et
- (c) les traitements de données dans des domaines du droit pénal effectués en vertu de conventions internationales, d'accords intergouvernementaux ou dans le cadre de la coopération avec l'Organisation internationale de police criminelle (OIPC – Interpol).

(2) Le contrôle et la surveillance des traitements mis en œuvre tant en application d'une disposition de droit interne qu'en application d'une convention internationale est exercé par une autorité de contrôle composée du Procureur Général d'Etat, ou de son délégué qui la préside, et de deux membres de la Commission nationale nommés, sur proposition de celle-ci, par le ministre.

L'organisation et le fonctionnement de l'autorité de contrôle font l'objet d'un règlement grand-ducal.

L'autorité de contrôle est informée immédiatement de la mise en œuvre d'un traitement de données visé par le présent article. Elle veille à ce que ces traitements soient effectués conformément aux dispositions légales qui les régissent.

Pour l'exercice de sa mission, l'autorité de contrôle a un accès direct aux données traitées. Elle peut procéder, quant aux traitements effectués, à des vérifications sur place et se faire communiquer tous renseignements et

documents utiles à sa mission. Elle peut également charger un de ses membres à procéder à des missions de contrôle spécifique qui sont exécutées dans les conditions indiquées ci-dessus. L'autorité de contrôle fait opérer les rectifications et radiations nécessaires. Elle présente chaque année au ministre un rapport rendant compte de l'exécution de sa mission.

Le droit d'accès aux données visées au présent article ne peut être exercé que par l'intermédiaire de l'autorité de contrôle. Celle-ci procède aux vérifications et investigations utiles, fait opérer les rectifications nécessaires et informe la personne concernée que le traitement en question ne contient aucune donnée contraire aux conventions, à la loi et à ses règlements d'exécution.

(3) Toute personne, agissant à titre privé, qui effectue un traitement en violation des dispositions du présent article est punie d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Chapitre IV. - Transferts de données vers des pays tiers

Art. 18. Principes

(1) Le transfert vers un pays tiers de données faisant l'objet d'un traitement ou destinées à faire l'objet d'un

traitement après leur transfert, ne peut avoir lieu que si le pays en question assure un niveau de protection adéquat et moyennant le respect des dispositions de la présente loi et de ses règlements d'exécution.

(2) Le caractère adéquat du niveau de protection offert par un pays tiers doit être apprécié par le responsable du traitement au regard de toutes les circonstances relatives à un transfert ou une catégorie de transferts de données, notamment la nature des données, la finalité et la durée du ou des traitements envisagés, le pays d'origine et le pays de destination finale, les règles de droit générales et sectorielles en vigueur dans le pays en cause, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées.

(3) En cas de doute, le responsable du traitement informe sans délai la Commission nationale qui apprécie si un pays tiers assure un niveau de protection adéquat. La Commission nationale notifie conformément à l'article 20 à la Commission européenne les cas dans lesquels elle estime que le pays tiers n'assure pas un niveau de protection adéquat.

(4) Lorsque la Commission européenne ou la Commission nationale constate qu'un pays tiers ne dispose pas d'un niveau de protection adéquat, tout transfert de données vers ce pays est prohibé.

(5) Quiconque effectue un transfert de données vers un pays tiers en violation des dispositions des paragraphes (1), (2) et (4) qui précèdent est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du transfert contraire aux dispositions des paragraphes (1), (2) et (4) du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 19. Dérogations

(1) Le transfert de données ou d'une catégorie de données vers un pays tiers n'assurant pas un niveau de protection adéquat au sens de l'article 18, paragraphe (2), peut toutefois être effectué à condition que:

- (a) la personne concernée ait donné son consentement au transfert envisagé, ou
- (b) le transfert soit nécessaire à l'exécution d'un contrat auquel la personne concernée et le responsable du traitement sont parties ou à l'exécution de mesures précontractuelles prises à la demande de la personne concernée, ou
- (c) le transfert soit nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers, ou
- (d) le transfert soit nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice, ou
- (e) le transfert soit nécessaire à la sauvegarde de l'intérêt vital de la personne concernée, ou
- (f) le transfert intervienne depuis un registre public tel que prévu à l'article 12, paragraphe (3) lettre (b).

(2) Dans le cas d'un transfert effectué vers un pays tiers n'assurant pas un niveau de protection adéquat au sens de l'article 18, paragraphe (2), le responsable du traitement doit notifier à la Commission nationale un rapport établissant les conditions dans lesquelles il a opéré le transfert.

(3) Sans préjudice des dispositions du paragraphe (1), la Commission nationale peut autoriser, sur la base d'une demande dûment motivée, un transfert ou un ensemble de transferts de données vers un pays tiers et n'assurant pas un niveau de protection adéquat, au sens de l'article 18, paragraphe (2), ceci lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes concernées, ainsi qu'à l'exercice des droits correspondants. Ces garanties peuvent résulter de clauses contractuelles appropriées. Le responsable du traitement est tenu de se conformer à la décision de la Commission nationale.

(4) Quiconque effectue un transfert de données vers un pays tiers en violation des dispositions du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du transfert contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 20. Information réciproque

(1) La Commission nationale informe le ministre de toute décision prise en application de l'article 18, paragraphes (3) et (4), et de l'article 19, paragraphes (1) et (2). Le ministre en informe la Commission européenne.

(2) Le ministre informe la Commission nationale de toute décision relative au niveau de protection d'un pays tiers prise par la Commission européenne.

Chapitre V. - Subordination et sécurité des traitements

Art. 21. Subordination

Toute personne qui agit sous l'autorité du responsable du traitement ou sous celle du sous-traitant, ainsi que le sous-traitant lui-même, et qui accède à des données ne peut les traiter que sur instruction du responsable du traitement, sauf en vertu d'obligations légales.

Art. 22. Sécurité des traitements

(1) Le responsable du traitement doit mettre en œuvre toutes les mesures techniques et l'organisation appropriées pour assurer la protection des données qu'il traite contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite. Ces mesures font l'objet d'un rapport annuel à soumettre par le responsable du traitement à la Commission nationale.

(2) Lorsque le traitement est mis en œuvre pour compte du responsable du traitement, celui-ci doit choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer. Il incombe au responsable du traitement ainsi qu'au sous-traitant de veiller au respect de ces mesures.

(3) Tout traitement effectué pour compte doit être régi par un contrat ou un acte juridique consigné par écrit qui lie le sous-traitant au responsable du traitement et qui prévoit notamment que:

- (a) le sous-traitant n'agit que sur la seule instruction du responsable du traitement; et que
- (b) les obligations visées au présent article incombent également à celui-ci.

Art. 23. Mesures de sécurité particulières

En fonction du risque d'atteinte à la vie privée, ainsi que de l'état de l'art et des coûts liés à leur mise en œuvre, les mesures visées à l'article 22, paragraphe (1) doivent:

- (a) empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement de données (contrôle à l'entrée des installations);
- (b) empêcher que des supports de données puissent être lus, copiés, modifiés ou déplacés par une personne non autorisée (contrôle des supports);
- (c) empêcher l'introduction non autorisée de toute donnée dans le système d'information, ainsi que toute prise de connaissance, toute modification ou tout effacement non autorisés de données enregistrées (contrôle de la mémoire);
- (d) empêcher que des systèmes de traitements de données puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données (contrôle de l'utilisation);
- (e) garantir que, pour l'utilisation d'un système de traitement automatisé de données, les personnes autorisées ne puissent accéder qu'aux données relevant de leur compétence (contrôle de l'accès);

- (f) garantir que puisse être vérifié et constaté l'identité des tiers auxquels des données peuvent être transmises par des installations de transmission (contrôle de la transmission);
- (g) garantir que puisse être vérifié et constaté a posteriori l'identité des personnes ayant eu accès au système d'information et quelles données ont été introduites dans le système, à quel moment et par quelle personne (contrôle de l'introduction);
- (h) empêcher que, lors de la communication de données et du transport de supports de données, les données puissent être lues, copiées, modifiées ou effacées de façon non autorisée (contrôle du transport);
- (i) sauvegarder les données par la constitution de copies de sécurité (contrôle de la disponibilité).

Art. 24. Secret professionnel

(1) Les membres de la Commission nationale et toute personne qui exerce des fonctions auprès de la Commission nationale ou accomplit une mission pour son compte ainsi que le chargé de la protection des données sont soumis au respect du secret professionnel prévu à l'article 458 du Code pénal, même après la fin de leur fonction.

(2) Le chargé de la protection des données agissant dans le cadre de l'accomplissement de ses missions, ne peut opposer à la Commission nationale le secret professionnel auquel il est soumis.

(3) Le prestataire de service de certification ne peut opposer à la Commission nationale le secret professionnel auquel il est soumis conformément à l'article 19 de la loi du 14 août 2000 relative au commerce électronique.

(4) Le responsable du traitement agissant dans le cadre de l'accomplissement de ses missions visées à l'article 7, paragraphe (1), ne peut opposer à la Commission nationale le secret professionnel auquel il est soumis lorsque celle-ci a été saisie conformément à l'article 32, paragraphes (4) et (5).

Art. 25. Sanctions relatives à la subordination et à la sécurité des traitements

Quiconque effectue un traitement en violation des règles relatives à la confidentialité ou à la sécurité visées aux articles 21, 22 et 23 est puni d'un emprisonnement de huit jours à six mois et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions des articles 21, 22 et 23 sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Chapitre VI. - Droits de la personne concernée

Art. 26. Le droit à l'information de la personne concernée

(1) Lorsque des données sont collectées directement auprès de la personne concernée, le responsable du traitement doit fournir à la personne concernée, au plus tard lors de la collecte et quels que soient les moyens et supports employés, les informations suivantes, sauf si la personne concernée en a déjà été informée:

- (a) l'identité du responsable du traitement et, le cas échéant, de son représentant;
- (b) la ou les finalités déterminées du traitement auquel les données sont destinées;
- (c) toute autre information supplémentaire telle que:
 - les destinataires ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées;
 - le fait de savoir si la réponse aux questions est obligatoire ou facultative ainsi que les conséquences éventuelles d'un défaut de réponse;
 - l'existence d'un droit d'accès aux données la concernant et de rectification de ces données;
 - la durée de conservation des données.

(2) Lorsque les données n'ont pas été collectées auprès de la personne concernée, le responsable du traitement doit, dès l'enregistrement des données ou, si une communication de données à un tiers est envisagée, au plus tard lors de la première communication de données, fournir à la personne concernée, sauf si elle en est déjà informée, les informations suivantes:

- (a) l'identité du responsable du traitement et, le cas échéant, de son représentant;
- (b) la ou les finalités déterminées du traitement auquel les données sont destinées;
- (c) toute information supplémentaire telle que:

- les catégories de données concernées;
- les destinataires ou les catégories de destinataires des données auxquels les données sont susceptibles d'être communiquées;
- l'existence d'un droit d'accès aux données la concernant et de rectification de ces données;
- la durée de conservation des données.

(3) Quiconque contrevient aux dispositions du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 27. Exceptions au droit à l'information de la personne concernée

(1) L'article 26, paragraphes (1) et (2), ne s'applique pas lorsque le traitement est nécessaire pour sauvegarder:

- (a) la sûreté de l'Etat;
- (b) la défense;
- (c) la sécurité publique;
- (d) la prévention, la recherche, la constatation et la poursuite d'infractions pénales y compris celles à la lutte contre le blanchiment, ou le déroulement de procédures judiciaires autres, au sens de l'article 8, paragraphe (1), et de l'article 17 de la présente loi;
- (e) un intérêt économique ou financier important de l'Etat ou de l'Union européenne, y compris dans les domaines monétaire, budgétaire et fiscal;
- (f) la protection de la personne concernée ou des droits et libertés d'autrui.

(2) Les dispositions de l'article 26 sont susceptibles de dérogations lors de la collecte de données dans les conditions prévues à l'article 9, paragraphe (1) lettre (c).

(3) Les dispositions de l'article 26 paragraphes (1) et (2) ne s'appliquent pas lorsque, en particulier pour un traitement ayant une finalité statistique, historique ou scientifique, l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés ou si l'enregistrement ou la communication des données est prévu par la loi.

(4) Quiconque contrevient aux dispositions des paragraphes (1) et (2) qui précèdent est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions des paragraphes (1) et (2) du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 28. Droit d'accès

(1) Sur demande à introduire auprès du responsable du traitement, la personne concernée ou ses ayants droit justifiant d'un intérêt légitime peuvent obtenir sans frais, à des intervalles raisonnables et sans délais excessifs:

- (a) l'accès aux données la concernant;
- (b) la confirmation que des données la concernant sont ou ne sont pas traitées, ainsi que des informations portant au moins sur les finalités du traitement, sur les catégories de données sur lesquelles il porte et les destinataires ou les catégories de destinataires auxquels les données sont communiquées;
- (c) la communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine des données;
- (d) la connaissance de la logique qui sous-tend tout traitement automatisé des données la concernant, au moins dans le cas des décisions automatisées visées à l'article 31.

(2) Celui qui entrave sciemment par quelque moyen que ce soit, l'exercice du droit d'accès, sera puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement.

(3) Le patient a un droit d'accès aux données le concernant. Le droit d'accès est exercé par le patient lui-même ou par l'intermédiaire d'un médecin qu'il désigne. En cas de décès du patient, son conjoint non séparé de corps et ses enfants ainsi que toute personne qui au moment du décès a vécu avec lui dans le ménage ou, s'il s'agit d'un mineur, ses père et mère, peuvent exercer, par l'intermédiaire d'un médecin qu'ils désignent, le droit d'accès dont question à l'alinéa qui précède.

Le droit d'accès du patient pourra encore être exercé, du vivant d'une personne placée sous le régime de la curatelle ou sous celui de la tutelle tel qu'il est organisé par la loi du 11 août 1982, par l'intermédiaire d'un médecin désigné par son curateur ou tuteur.

(4) Toute personne a un droit d'accès aux données la concernant et utilisées aux fins d'un traitement mis en œuvre dans le cadre de la liberté d'expression tel que prévu à l'article 9. Aussi longtemps que les données auxquelles l'accès est demandé n'ont pas été publiées, la communication de ces données, ainsi que toute information disponible sur leur origine ne peut se faire que par l'intermédiaire de la Commission nationale.

(5) Selon le cas, le responsable du traitement procédera à la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la présente loi, notamment en raison du caractère incomplet ou inexact des données, sous peine d'encourir dans les conditions de l'article 33 l'interdiction temporaire ou définitive du traitement ou la destruction des données.

(6) Toute personne qui dans l'exercice de son droit d'accès a des raisons sérieuses d'admettre que les données qui lui ont été communiquées ne sont pas conformes aux données traitées, peut en informer la Commission nationale qui procède aux vérifications nécessaires.

(7) Toute rectification, tout effacement ou verrouillage effectué conformément au paragraphe (5) sera notifié sans délai par le responsable du traitement aux destinataires auxquels les données ont été communiquées, à moins que cela ne s'avère impossible.

(8) Sans préjudice de la sanction prévue au paragraphe (5), quiconque contrevient sciemment aux dispositions du présent article ou quiconque prend sciemment un nom ou prénom supposé ou une fausse qualité pour obtenir communication des données faisant l'objet d'un traitement en application du paragraphe (1), est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement.

Art. 29. Exceptions au droit d'accès

(1) Le responsable du traitement peut limiter ou différer l'exercice du droit d'accès d'une personne concernée lorsqu'une telle mesure est nécessaire pour sauvegarder:

- (a) la sûreté de l'Etat;
- (b) la défense;
- (c) la sécurité publique;
- (d) la prévention, la recherche, la constatation et la poursuite d'infractions pénales y compris celles à la lutte contre le blanchiment, ou le déroulement de procédures judiciaires autres, au sens de l'article 8, paragraphe (1), et de l'article 17 de la présente loi;
- (e) un intérêt économique ou financier important de l'Etat ou de l'Union européenne, y compris dans les domaines monétaire, budgétaire et fiscal;
- (f) la protection de la personne concernée ou des droits et libertés d'autrui;
- (g) la liberté d'expression et que la mesure d'exception est prise conformément à l'article 28, paragraphe (4);
- (h) une mission de contrôle, d'inspection ou de réglementation relevant, même à titre occasionnel, de l'exercice de l'autorité publique, dans les cas visés aux points (c), (d) et (e).

(2) Au cas où il n'existe manifestement aucun risque d'atteinte à la vie privée d'une personne concernée, le responsable du traitement peut limiter le droit d'accès lorsque les données sont traitées exclusivement aux fins de recherche scientifique ou sont stockées sous la forme de données pendant une durée n'excédant pas celle nécessaire à la seule finalité d'établissement de statistiques et que ces données ne puissent être utilisées aux fins de prendre une mesure ou une décision se rapportant à des personnes précises.

(3) Le responsable du traitement doit indiquer le motif pour lequel il limite ou diffère l'exercice du droit d'accès.

Lorsque le droit d'accès est différé, le responsable du traitement doit indiquer la date à partir de laquelle le droit d'accès peut à nouveau être exercé. Le responsable du traitement notifiera le motif à la Commission nationale.

(4) En cas de limitation de l'exercice du droit d'accès de la personne concernée, le droit d'accès est exercé par la Commission nationale qui dispose d'un pouvoir d'investigation en la matière et qui fait opérer la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la

présente loi. La Commission nationale peut communiquer à la personne concernée le résultat de ses investigations, sans toutefois mettre en danger la ou les finalités des traitements en question.

(5) Quiconque contrevient à la disposition du paragraphe (3) qui précède est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement.

Art. 30. Droit d'opposition de la personne concernée

(1) Toute personne concernée a le droit:

- (a) de s'opposer à tout moment pour des raisons prépondérantes et légitimes tenant à sa situation particulière, à ce que des données la concernant fassent l'objet d'un traitement, sauf en cas de dispositions légales prévoyant expressément le traitement. En cas d'opposition justifiée, le traitement mis en œuvre par le responsable du traitement ne peut pas porter sur ces données;
- (b) de s'opposer, sur demande et gratuitement, au traitement la concernant envisagé par le responsable du traitement à des fins de prospection; il incombe au responsable du traitement de porter l'existence de ce droit à la connaissance de la personne concernée;
- (c) d'être informée avant que des données la concernant ne soient pour la première fois communiquées à des tiers ou utilisées pour le compte de tiers à des fins de prospection et de se voir expressément offrir le droit de s'opposer, gratuitement, à ladite communication ou utilisation.

(2) Quiconque contrevient sciemment aux dispositions du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement.

Art. 31. Décisions individuelles automatisées

Une personne peut être soumise à une décision individuelle automatisée produisant des effets juridiques à son égard, si cette décision:

- (a) est prise dans le cadre de la conclusion ou de l'exécution d'un contrat, à condition que la demande de conclusion ou d'exécution du contrat, introduite par la personne concernée, ait été satisfaite ou que des mesures appropriées, telle que la possibilité de faire valoir son point de vue, garantissent la sauvegarde de son intérêt légitime, ou
- (b) est autorisée par la loi, qui précise les mesures garantissant la sauvegarde de l'intérêt légitime de la personne concernée.

Chapitre VII. - Contrôle et surveillance de l'application de la loi

Art. 32. Missions et pouvoirs de la Commission nationale

(1) Il est institué une autorité de contrôle dénommée «Commission nationale pour la protection des données» chargée de contrôler et de vérifier si les données soumises à un traitement sont traitées en conformité avec les dispositions de la présente loi et de ses règlements d'exécution.

(2) Tous les ans, la Commission nationale rend compte, dans son rapport écrit aux membres du Gouvernement en conseil, de l'exécution de ses missions. Dans ce rapport, elle relève plus particulièrement l'état des notifications et des autorisations, les déficiences ou abus qui ne sont pas spécifiquement visés par les dispositions légales, réglementaires et administratives existantes. Elle publiera son rapport annuel. Le rapport est avisé par la commission consultative des droits de l'homme, organe consultatif du gouvernement en matière de droits de l'homme sur le territoire du Grand-Duché de Luxembourg dont la composition et les attributions sont déterminées par règlement grand-ducal.

(3) Les missions de la Commission nationale sont les suivantes:

- (a) assurer l'application des dispositions de la présente loi et de ses règlements d'exécution en particulier celles relatives à la confidentialité et à la sécurité des traitements;
- (b) recevoir les notifications préalables à la mise en œuvre d'un traitement, de même que les changements affectant le contenu de ces notifications, et procéder a posteriori au contrôle de la licéité des traitements notifiés; de même elle est informée sans délai de tout traitement soumis à autorisation préalable;
- (c) assurer la publicité des traitements lui notifiés en tenant un registre afférent, sauf disposition contraire;
- (d) autoriser la mise en œuvre des traitements soumis au régime de l'article 14 de la présente loi;
- (e) être demandée en son avis sur tous les projets ou propositions de loi portant création d'un traitement de même que sur toutes les mesures réglementaires ou administratives émises sur base de la présente loi. Ces avis sont publiés au rapport annuel visé à l'article 15, paragraphe (6);

- (f) présenter au Gouvernement toutes suggestions susceptibles de simplifier et d'améliorer le cadre législatif et réglementaire à l'égard du traitement des données;
- (g) recevoir et le cas échéant après discussion avec les auteurs approuver les codes de conduite relatifs à un traitement ou un ensemble de traitements lui soumis par des associations professionnelles représentatives de responsables du traitement;
- (h) conseiller le Gouvernement, soit à la demande de celui-ci, soit sur sa propre initiative, au sujet des conséquences de l'évolution des technologies de traitement de l'information au regard du respect des libertés et droits fondamentaux des personnes; à cette fin, elle peut faire procéder à des études, des enquêtes ou expertises;
- (i) favoriser de façon régulière et par tout moyen qu'elle juge opportun, la diffusion d'informations relatives aux droits des personnes concernées et aux obligations des responsables du traitement, notamment en ce qui concerne le transfert de données vers des pays tiers.

(4) La Commission nationale peut être saisie par toute personne, agissant par elle-même, par l'entremise de son avocat ou par toute autre personne physique ou morale dûment mandatée, d'une demande relative au respect de ses droits et libertés fondamentaux à l'égard d'un traitement. La personne concernée est informée des suites réservées à sa requête.

(5) La Commission nationale peut, en particulier, être saisie par toute personne concernée d'une demande de vérification de la licéité d'un traitement en cas de refus ou de limitation de l'exercice du droit d'accès de la personne concernée conformément à l'article 29, paragraphe (4), de la présente loi.

(6) Si la Commission nationale est saisie par l'une des personnes ou organes visés à l'article 11, paragraphe (2), sur une violation de cet article, elle statue dans le mois de la saisine.

(7) Dans le cadre de la présente loi, la Commission nationale dispose d'un pouvoir d'investigation en vertu duquel elle a accès aux données faisant l'objet du traitement en question. Elle recueille toutes les informations nécessaires à l'accomplissement de sa mission de contrôle. A cette fin elle a un accès direct aux locaux autres que les locaux d'habitation où a lieu le traitement ainsi qu'aux données faisant l'objet du traitement et procède aux vérifications nécessaires.

(8) La Commission nationale a le droit d'ester en justice dans l'intérêt de la présente loi et de ses règlements d'exécution. Elle dénonce aux autorités judiciaires les infractions dont elle a connaissance.

(9) La Commission nationale coopère avec ses homologues que sont les autorités de contrôle instituées dans les autres Etats membres de l'Union européenne, dans la mesure nécessaire à l'accomplissement de leurs missions notamment en échangeant toutes informations utiles.

(10) La Commission nationale représente le Luxembourg au «groupe de protection des personnes à l'égard du traitement des données à caractère personnel» institué par l'article 29 de la Directive 95/46/CE.

(11) Quiconque empêche ou entrave sciemment, de quelque manière que ce soit, l'accomplissement des missions incombant à la Commission nationale, est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. Est considéré comme empêchant ou entravant sciemment l'accomplissement des missions incombant à la Commission nationale, le refus opposé à ses membres de donner accès aux locaux autres que les locaux d'habitation, où a lieu un traitement aux données faisant l'objet d'un traitement ou de communiquer tous renseignements et documents demandés.

Art. 33. Sanctions administratives

(1) La Commission nationale peut prendre les sanctions disciplinaires suivantes:

- (a) avertir ou admonester le responsable du traitement ayant violé les obligations lui imposées par les articles 21 à 24;
- (b) verrouiller, effacer ou détruire des données faisant l'objet d'un traitement contraire aux dispositions de la présente loi ou de ses règlements d'exécution;
- (c) interdire temporairement ou définitivement un traitement contraire aux dispositions de la présente loi ou à ses règlements d'exécution;
- (d) ordonner l'insertion intégrale ou par extraits de la décision d'interdiction par la voie des journaux ou de toute autre manière, aux frais de la personne sanctionnée.

(2) Les décisions ci-dessus sont susceptibles d'un recours en réformation suivant l'article 3 de la loi du 7 novembre 1996 portant organisation des juridictions de l'ordre administratif.

Art. 34. Composition de la Commission nationale

(1) La Commission nationale est une autorité publique qui prend la forme d'un établissement public. Son siège est fixé à Luxembourg-ville. Il peut être transféré à tout moment dans toute autre localité du Luxembourg par voie de règlement grand-ducal.

La Commission nationale dispose de la personnalité juridique et jouit de l'autonomie financière et administrative, sous la tutelle du ministre.

Elle exerce en toute indépendance les missions dont elle est investie en vertu de la présente loi.

(2) La Commission nationale est composée de trois membres effectifs et de trois membres suppléants nommés et révoqués par le Grand-Duc sur proposition du Gouvernement en conseil. Le président est désigné par le Grand-Duc.

Les membres sont nommés pour un terme de six ans, renouvelable une fois.

Le Gouvernement en conseil propose au Grand-Duc comme membre effectif et suppléant chaque fois au moins un juriste et un informaticien justifiant d'une formation universitaire accomplie.

Avant d'entrer en fonction, le président de la Commission nationale prête entre les mains du Grand-Duc ou de son représentant le serment suivant: «Je jure fidélité au Grand-Duc, obéissance à la constitution et aux lois de l'Etat. Je promets de remplir mes fonctions avec intégrité, exactitude et impartialité.»

Avant d'entrer en fonction, les membres de la Commission nationale prêtent entre les mains du président de la Commission nationale le serment suivant: «Je jure fidélité au Grand-Duc, obéissance à la constitution et aux lois de l'Etat. Je promets de remplir mes fonctions avec intégrité, exactitude et impartialité.»

Lorsque le président ou un membre effectif de la Commission nationale est issu du secteur public, il obtient un congé spécial pour la durée de son mandat avec maintien de tous les avantages et droits découlant de son statut respectif. Il continue notamment à jouir de son traitement, indemnité ou salaire suivant le cas, ainsi que du régime de sécurité sociale correspondant à son statut.

En cas de cessation du mandat, il est réintégré sur sa demande dans son administration d'origine à un emploi correspondant au traitement qu'il a touché précédemment, augmenté des échelons et majorations de l'indice se rapportant aux années de service passées comme président ou membre effectif jusqu'à concurrence du dernier échelon du grade.

A défaut de vacance, il peut être créé un emploi hors cadre correspondant à ce traitement; cet emploi est supprimé de plein droit à la première vacance qui se produit dans une fonction appropriée du cadre normal.

Lorsque le président ou un membre effectif de la Commission nationale est issu du secteur privé, il touche une rémunération calculée par référence à la réglementation fixant le régime des indemnités des employés occupés dans les administrations et services de l'Etat qui est applicable en la matière, sur base d'une décision individuelle prise en vertu de l'article 23 du règlement grand-ducal du 28 juillet 2000 fixant le régime des indemnités des employés occupés dans les administrations et services de l'Etat. Il reste affilié au régime de sécurité sociale auquel il était soumis pendant l'exercice de sa dernière occupation.

En cas de cessation du mandat, il touche pendant une durée maximale d'un an une indemnité d'attente mensuelle correspondant au salaire ou traitement mensuel moyen du dernier revenu professionnel cotisable annuel mis en compte au titre de sa carrière d'assurance en cours avant le début de sa fonction de président ou de membre effectif de la Commission nationale. Cette indemnité d'attente est réduite dans la mesure où l'intéressé touche un revenu professionnel ou bénéficie d'une pension personnelle.

Le président et les membres effectifs de la Commission nationale bénéficient d'une indemnité spéciale tenant compte de l'engagement requis par les fonctions, à fixer par règlement grand-ducal.

La démission d'un membre de la Commission nationale intervient de plein droit par l'atteinte de la limite d'âge de 65 ans.

Les membres suppléants touchent une indemnité dont le montant est fixé par règlement grand-ducal.

(3) Les membres de la Commission nationale ne peuvent être membre du Gouvernement, de la Chambre des Députés, du Conseil d'Etat ou du Parlement Européen ni exercer d'activité professionnelle ou détenir directement ou indirectement des intérêts dans une entreprise ou tout autre organisme opérant dans le champ des traitements de données.

(4) Si, en cours de mandat un membre de la Commission nationale cesse d'exercer ses fonctions, le mandat de son successeur est limité à la période restant à courir.

Art. 35. Fonctionnement de la Commission nationale

(1) La Commission nationale est un organe collégial. Elle établit son règlement intérieur comprenant ses procédures et méthodes de travail dans le mois de son installation. Le règlement intérieur est publié au Mémorial.

(2) Sous réserve des dispositions de la présente loi, le règlement intérieur fixe:

- (a) les règles de procédure applicables devant la Commission nationale,
- (b) les conditions de fonctionnement de la Commission nationale,
- (c) l'organisation des services de la Commission nationale.

(3) Les membres effectifs de la Commission nationale sont convoqués par le président. La convocation est de droit à la demande de deux membres effectifs. La convocation précise l'ordre du jour.

Les membres effectifs empêchés d'assister à une réunion sont tenus d'en avvertir leur suppléant et de lui continuer la convocation.

(4) La Commission nationale ne peut valablement siéger ni délibérer qu'à condition de réunir trois membres.

(5) Les membres de la Commission nationale ne peuvent siéger, délibérer ou décider dans aucune affaire dans laquelle ils ont un intérêt direct ou indirect.

(6) Les délibérations sont prises à la majorité des voix. Les abstentions ne sont pas recevables.

(7) Le Gouvernement en conseil ayant proposé à la nomination un membre de la Commission nationale peut proposer sa révocation au Grand-Duc. La Commission nationale est entendue en son avis avant toute révocation.

(8) Dans l'exercice de leurs fonctions, les membres et les suppléants de la Commission nationale ne reçoivent d'instruction d'aucune autorité.

Art. 36. Statut des membres et agents de la Commission nationale

(1) Le cadre du personnel de la Commission nationale comprend les fonctions et emplois suivants:

Dans la carrière moyenne de l'administration, grade de computation de la bonification d'ancienneté :
grade 7, carrière du rédacteur :

- des inspecteurs principaux 1^{er} en rang
- des inspecteurs principaux
- des inspecteurs
- des chefs de bureau
- des chefs de bureau adjoints
- des rédacteurs principaux
- des rédacteurs

Les agents de la carrière moyenne des rédacteurs sont des fonctionnaires de l'Etat en ce qui concerne notamment leur statut, leur traitement et leur régime de pension qui est régi par les dispositions légales régissant les fonctionnaires de l'Etat.

(2) Le cadre prévu au paragraphe (1) ci-dessus peut être complété par des employés de l'Etat ainsi que par des ouvriers de l'Etat dans les limites des crédits disponibles.

La rémunération des employés de l'Etat est fixée conformément au règlement grand-ducal du 28 juillet 2000 fixant le régime des indemnités des employés occupés dans les administrations et services de l'Etat.

(3) Les rémunérations et autres indemnités de tous membres, agents et employés de la Commission nationale sont à charge de la Commission nationale.

(4) La Commission nationale peut, dans des cas déterminés, faire appel à des experts externes dont les prestations sont définies et rémunérées sur la base d'un contrat de droit privé.

Art. 37. Dispositions financières

(1) Au moment de sa création, la Commission nationale bénéficie d'une dotation initiale de deux cent mille euros à charge du budget de l'Etat. L'Etat met à sa disposition les biens mobiliers et immobiliers nécessaires au bon fonctionnement et à l'exercice de ses missions.

(2) L'exercice financier de la Commission nationale coïncide avec l'année civile.

(3) Avant le 31 mars de chaque année, la Commission nationale arrête son compte d'exploitation de l'exercice précédent, ensemble avec son rapport de gestion. Avant le 30 septembre de chaque exercice, la Commission nationale arrête le budget pour l'exercice à venir. Le budget, les comptes annuels et les rapports arrêtés sont transmis au Gouvernement en conseil qui décide de la décharge à donner à la Commission nationale. La décision constatant la décharge accordée à la Commission nationale ainsi que les comptes annuels de la Commission nationale sont publiés au Mémorial.

(4) La Commission nationale est autorisée à prélever la contrepartie de ses frais du personnel en service et de ses frais de fonctionnement par la redevance à percevoir telle que prévue à l'article 13 de la présente loi. Pour le solde des frais restant à couvrir dans le cadre de ses missions conférées par la présente loi, la Commission nationale bénéficiera d'une dotation d'un montant à déterminer sur une base annuelle et à inscrire au budget de l'Etat.

(5) La loi du 27 novembre 2001 concernant le budget des recettes et des dépenses de l'Etat pour l'exercice 2002 est modifiée comme suit:

il est ajouté au budget des dépenses au Chapitre III – Dépenses courantes sous «00 – Ministère d'Etat» une section «00.9 Commission nationale pour la protection des données» émergeant les articles suivants:

«12.300: Prise en charge par l'Etat des frais encourus par la Commission nationale pour la protection des données. (crédit non limitatif et sans distinction d'exercice) 200.870
33.000: Dotation initiale en faveur de la Commission nationale pour la protection des données . . 200.000»

Chapitre VIII. - Recours juridictionnels

Art. 38. Généralités

Sans préjudice des sanctions pénales instituées par la présente loi et des actions en responsabilité régies par le droit commun, en cas de mise en œuvre d'un traitement en violation des formalités prévues par la présente loi toute personne dispose d'un recours juridictionnel tel que prévu ci-après:

Art. 39. Action en cessation

(1) A la requête

- du Procureur d'Etat qui a déclenché une action publique pour violation de la présente loi,
- de la Commission nationale, dans l'hypothèse où une sanction disciplinaire visée à l'article 33 de la présente loi, qui n'a pas fait l'objet d'un recours ou qui a été confirmée par la juridiction administrative, n'a pas été respectée, ou
- d'une personne lésée, dans l'hypothèse où la Commission nationale n'a pas pris position sur une saisine intervenue sur la base de l'article 32, paragraphe (4), (5) ou (6) de la présente loi,

le président du tribunal d'arrondissement du lieu où le traitement est mis en œuvre, ou le juge qui le remplace, ordonne la cessation du traitement contraire aux dispositions de la présente loi et la suspension provisoire de l'activité du responsable du traitement ou du sous-traitant. Le président du tribunal d'arrondissement, ou le juge qui le remplace, peut ordonner la fermeture provisoire de l'établissement du responsable du traitement ou du sous-traitant lorsque sa seule activité est de traiter des données.

(2) L'action est recevable même lorsque le traitement illégal a pris fin ou n'est plus susceptible de se reproduire.

(3) L'action est introduite et jugée comme en matière de référé conformément aux articles 932 à 940 du Nouveau code de procédure civile. Toutefois, par dérogation à l'article 939, alinéa 2, du Nouveau code de procédure civile, l'ordonnance de référé n'est pas susceptible d'opposition.

(4) Sont également applicables les articles 2059 à 2066 du Code civil.

(5) La publication de la décision peut être ordonnée, en totalité ou par extrait, aux frais du contrevenant, par la voie des journaux ou de toute autre manière. Il ne peut être procédé à la publication qu'en vertu d'une décision judiciaire coulée en force de chose jugée.

(6) La suspension provisoire et le cas échéant la fermeture provisoire peuvent être ordonnées indépendamment de l'action publique. La suspension provisoire ou la fermeture provisoire ordonnée par le président du tribunal d'arrondissement, ou par le juge qui le remplace, prend toutefois fin en cas de décision de non-lieu ou d'acquiescement, et au plus tard à l'expiration d'un délai de deux ans à partir de la décision initiale de suspension ou de fermeture.

Chapitre IX. - Le chargé de la protection des données

Art. 40. Le chargé de la protection des données

(1) Tout responsable de traitement peut, dans le cadre de l'article 12, paragraphe (3) sous (a), et aux fins y visées, désigner un chargé de la protection des données, dont il communique l'identité à la Commission nationale.

(2) Les pouvoirs du chargé de la protection des données sont les suivants:

- (a) un pouvoir d'investigation aux fins d'assurer la surveillance du respect des dispositions de la présente loi et de ses règlements d'exécution par le responsable du traitement;
- (b) un droit d'information auprès du responsable du traitement et corrélativement, un droit d'informer le responsable du traitement des formalités à accomplir afin de se conformer aux dispositions de la présente loi et de ses règlements d'exécution.

(3) Dans l'exercice de ses missions le chargé de la protection des données est indépendant vis-à-vis du responsable du traitement qui le désigne:

- (a) il ne connaît aucun lien de subordination vis-à-vis du responsable du traitement et ne peut être lié au responsable du traitement par un contrat de travail;
- (b) il ne peut être révoqué pour des raisons liées à l'exercice de ses missions, hormis le cas de la violation de ses obligations légales ou conventionnelles.

(4) Le chargé de la protection consulte la Commission nationale en cas de doute quant à la conformité à la présente loi d'un traitement mis en œuvre sous sa surveillance.

(5) Peuvent être désignés à la fonction de chargé de la protection des données les personnes physiques et morales qui sont agréées par la Commission nationale.

(6) L'agrément pour l'activité du chargé de la protection des données est subordonné à la justification d'une formation universitaire accomplie en droit, économie, gestion d'entreprise, sciences de la nature, ou informatique ainsi que d'assises financières d'une valeur de 20.000 euros.

(7) Par dérogation au paragraphe précédent, les membres inscrits dans une des professions réglementées suivantes peuvent être agréés comme chargé de la protection des données sans autre condition: avocat à la Cour, réviseur d'entreprises, expert-comptable, médecin.

Un règlement grand-ducal peut ajouter à cette liste d'autres professions réglementées et assujetties à un organisme de surveillance ou de discipline, soit officiel soit propre à la profession et reconnu par la loi.

(8) La Commission nationale vérifie les qualités de tout chargé de la protection des données. Elle peut s'opposer à tout moment à la désignation ou au maintien du chargé de la protection des données lorsqu'il:

- (a) ne présente pas les qualités requises pour la fonction de chargé de la protection des données; ou
- (b) est d'ores et déjà en relation avec le responsable du traitement dans le cadre d'autres activités que celle du traitement des données et que cette relation fait naître un conflit d'intérêts limitant son indépendance.

En cas d'opposition de la Commission nationale, le responsable du traitement dispose de trois jours pour désigner un nouveau chargé de la protection des données.

(9) La Commission nationale définit les modalités du contrôle continu des qualités requises à la fonction de chargé de la protection des données.

(10) Un règlement grand-ducal fixera les modalités de désignation et de révocation du chargé de protection des données, d'exécution de ses missions, de même que ses relations avec la Commission nationale.

Chapitre X. - Dispositions spécifiques, transitoires et finales

Art. 41. Dispositions spécifiques

- (1) (a) Les autorités compétentes visées aux articles 88-1 à 88-4 du Code d'instruction criminelle, et
- (b) les autorités agissant dans le cadre d'un crime flagrant ou dans le cadre de l'article 40 du Code d'instruction criminelle, accèdent de plein droit, sur requête et par l'intermédiaire de l'Institut luxembourgeois de régulation (ci-après «ILR») aux données concernant l'identité des abonnés et utilisateurs

des opérateurs et fournisseurs de communications électroniques ainsi que des services postaux et des fournisseurs de ces services.

La centrale des secours d'urgence 112 et la centrale du service d'incendie et de sauvetage de la Ville de Luxembourg accèdent dans les mêmes conditions et modalités que les autorités visées à l'alinéa précédent aux seules données concernant l'identité des abonnés et utilisateurs des opérateurs et fournisseurs de communications électroniques.

(2) A ces fins, les opérateurs et les fournisseurs mettent d'office et gratuitement à la disposition de l'ILR les données prescrites au paragraphe (1). Les données doivent être actualisées au moins une fois par jour. L'accès doit être garanti vingt-quatre heures sur vingt-quatre et sept jours sur sept. Un règlement grand-ducal détermine les services de communications électroniques et services postaux pour lesquels les opérateurs et fournisseurs de services doivent mettre à disposition les données ainsi que la nature, le format et les modalités de mise à disposition des données.

(3) L'accès de plein droit se limite aux mesures spéciales de surveillance telles que prévues aux articles 88-1 à 88-4 du Code d'instruction criminelle, celles prises en matière de crime flagrant ou dans le cadre de l'article 40 du Code d'Instruction criminelle et aux mesures particulières de secours d'urgence prestées dans le cadre des activités de la centrale des secours d'urgence 112 et de la centrale du service d'incendie et de sauvetage de la Ville de Luxembourg.

(4) La procédure est entièrement automatisée suite à l'autorisation de la Commission nationale. La Commission nationale vérifiera en particulier la sécurisation du système informatique utilisé. Cette automatisation permettra l'accès à distance par voie de communication électronique.

Art. 42. Dispositions transitoires

(1) Les traitements existant dans des fichiers non automatisés ou automatisés antérieurs à l'entrée en vigueur de la présente loi doivent être rendus conformes aux dispositions du chapitre II et du chapitre VI, dans un délai de deux ans à compter de la date d'entrée en vigueur de la présente loi.

(2) Toutefois la personne concernée peut obtenir, sur demande, et notamment en ce qui concerne l'exercice de son droit d'accès, la rectification, l'effacement ou le verrouillage des données incomplètes, inexactes ou conservées de manière incompatible aux fins légitimes poursuivies par le responsable du traitement.

(3) La Commission nationale peut permettre que les données conservées uniquement à des fins de recherche historiques soient dispensées de respecter le paragraphe (1).

Art. 43. Mise en vigueur des dispositions transitoires

(1) La Commission nationale établira le schéma de notification prévu à l'article 13, paragraphe (3), dans les quatre mois de la nomination de ses membres. Elle informera le public, moyennant publication au Mémorial et communiqué de presse aux journaux édités au Luxembourg, de la date à partir de laquelle le schéma de notification est disponible auprès de la Commission nationale.

(2) Les responsables du traitement procéderont à la notification de leurs traitements dans les quatre mois à partir de la date de la publication officielle mentionnée au paragraphe (1).

(3) Les responsables du traitement dont les traitements sont autorisés, lors de l'entrée en vigueur de la présente loi, moyennant règlement grand-ducal ou arrêté ministériel «autorisant la création et l'exploitation d'une banque de données», ne notifieront ou ne demanderont l'autorisation de leurs traitements qu'à l'expiration de la durée de validité de l'autorisation octroyée, à moins que pour des raisons de conformité avec les dispositions de la présente loi, ils jugent nécessaire de le faire auparavant.

(4) Les traitements non automatisés de données contenues ou appelées à figurer dans un fichier sont à notifier dans les douze mois à partir de la date de la publication officielle mentionnée au paragraphe (1).

Art. 44. Dispositions finales

(1) La loi modifiée du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques est abrogée.

(2) Pour autant qu'ils ne sont pas contraires aux dispositions de la présente loi, les règlements pris en exécution de la loi modifiée du 31 mars 1979 précitée resteront en vigueur tant qu'ils n'auront pas été remplacés par de nouvelles dispositions.

Art. 45. Entrée en vigueur

La présente loi entre en vigueur le premier jour du quatrième mois qui suit sa publication au Mémorial. Par dérogation à ce qui précède, les articles 34, 35, 36 et 37 entrent en vigueur trois jours après publication de la présente loi au Mémorial.

Projet de loi n° 5181 du 11 juillet 2003 relatif aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques et portant modification des articles 88-2 et 88-4 du Code d'instruction criminelle, et de la loi du 2 août 2002 relative à la protection de la personne à l'égard du traitement des données à caractère personnel.

TEXTE DU PROJET DE LOI

Art. 1^{er}.– Champ d'application

Sans préjudice de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel et de la législation sur les réseaux et les services de communications électroniques; les dispositions spécifiques de la présente loi s'appliquent au traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux de communications publics.

Art. 2.– Définitions

Aux fins de la présente loi on entend par:

(a) «abonné»: une personne physique ou morale partie à un contrat avec une entreprise offrant des services de communications électroniques accessibles au public, pour la fourniture de tels services;

(b) «appel»: une connexion établie au moyen d'un service téléphonique accessible au public permettant une communication bidirectionnelle en temps réel;

(c) «consentement»: toute manifestation de volonté expresse, non équivoque, libre, spécifique et informée par laquelle l'utilisateur ou l'abonné accepte que les données à caractère personnel fassent l'objet d'un traitement;

(d) «communication»: toute information échangée ou acheminée entre un nombre fini de parties au moyen d'un service de communications électroniques accessible au public à l'exception des informations qui sont acheminées dans le cadre d'un service de radiodiffusion au public par l'intermédiaire d'un réseau de communications électroniques sauf si et dans la mesure où un lien peut être établi entre l'information et l'abonné ou l'utilisateur identifiable qui la reçoit;

(e) «courrier électronique»: tout message sous forme de texte, de voix, de son ou d'image envoyé par un réseau de communications public, qui peut être stocké dans le réseau ou dans l'équipement terminal du destinataire jusqu'à ce que ce dernier le récupère;

(f) «données relatives au trafic»: toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation;

(g) «données de localisation»: toutes les données traitées dans un réseau de communications électroniques qui comportent des indications sur la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public;

(h) «réseau de communications électroniques»: les systèmes de transmission et, le cas échéant, les équipements de commutation ou de routage et les autres ressources qui permettent l'acheminement de signaux par câble, par voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques comprenant les réseaux satellitaires, les réseaux terrestres fixes (avec commutation de circuits ou de paquets, y compris l'Internet) et mobiles, les systèmes utilisant le réseau électrique, pour autant qu'ils servent à la transmission de signaux, les réseaux utilisés pour la radiodiffusion sonore et télévisuelle et les réseaux câblés de télévision, quel que soit le type d'information transmise;

(i) «réseau de communications public»: un réseau de communications électroniques utilisé entièrement ou principalement pour la fourniture de services de communications électroniques accessibles au public. Le fournisseur du réseau de communications public est dénommé ci-après «opérateur»;

(j) «service de communications électroniques»: un service fourni normalement contre rémunération qui consiste entièrement ou principalement en la transmission de signaux sur les réseaux de communications électroniques, y compris les services de télécommunications et les services de transmission sur les réseaux utilisés pour la radiodiffusion, mais qui exclut les services consistant à fournir des contenus à l'aide de réseaux et de services de communications électroniques ou à exercer une responsabilité éditoriale sur ces contenus; il ne comprend pas les services de la société de l'information qui ne consistent pas entièrement

ou principalement en la transmission de signaux sur des réseaux de communications électroniques. Le fournisseur de services de communications électroniques est dénommé ci-après «fournisseur de services»;

(k) «service à valeur ajoutée»: tout service qui exige le traitement de données relatives au trafic ou à la localisation, à l'exclusion des données qui ne sont pas indispensables pour la transmission d'une communication ou sa facturation;

(l) «utilisateur»: une personne physique ou morale qui utilise ou demande un service de communications électroniques accessible au public;

(m) «utilisateur final» un utilisateur qui ne fournit pas de réseaux de communications publics ou de services de communications électroniques accessibles au public.

Art. 3.– Sécurité

(1) Le fournisseur de services prend les mesures techniques et d'organisation appropriées afin de garantir la sécurité de ses services, le cas échéant conjointement avec l'opérateur en ce qui concerne la sécurité du réseau. En cas d'atteinte ou de risque d'atteinte grave à la sécurité du réseau et/ou des services, le fournisseur de services et le cas échéant l'opérateur prend les mesures appropriées pour y remédier, les frais étant à sa seule charge.

(2) Sous réserve de ce qui précède, le fournisseur de services et le cas échéant l'opérateur informe ses abonnés de tout risque imminent d'atteinte à la sécurité du réseau et/ou des services mettant en cause la confidentialité des communications ainsi que du moyen éventuel pour y remédier, y compris du coût probable que cela implique.

Art. 4.– Confidentialité des communications

(1) Tout fournisseur de services et/ou opérateur assure la confidentialité des communications effectuées au moyen d'un réseau de communications public et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes.

(2) Il est interdit à toute personne autre que l'abonné, l'utilisateur ou l'utilisateur final concerné d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement de l'abonné, de l'utilisateur ou de l'utilisateur final concerné.

(3) Le paragraphe (2):

(a) n'empêche pas le stockage technique nécessaire à l'acheminement d'une communication, sans préjudice du principe de confidentialité;

(b) ne s'applique pas aux autorités agissant dans le cadre d'un crime flagrant ou dans le cadre de l'article 40 du Code d'instruction criminelle et celles compétentes en vertu des articles 88-1 à 88-4 du Code d'instruction criminelle conformément aux législations en vigueur pour sauvegarder la sûreté de l'Etat, la défense, la sécurité publique et pour la prévention, la recherche, la constatation et la poursuite des infractions pénales;

(c) ne s'applique pas aux communications et aux données relatives au trafic y afférentes, effectuées à destination du numéro d'appel d'urgence unique européen 112 et des numéros d'urgence déterminés par l'Institut dans le seul but de permettre (a) la réécoute de messages lors de problèmes de compréhension ou d'ambiguïté entre l'appelant et l'appelé, (b) la documentation de fausses alertes, de menaces et d'appels abusifs et (c) la production de preuves lors de contestation sur le déroulement d'actions de secours.

Les données relatives au trafic y afférentes dont les données de localisation sont à effacer une fois le secours apporté. Le contenu des communications est à effacer après un délai de 6 mois,

(d) n'affecte pas l'enregistrement légalement autorisé de communications et des données relatives au trafic y afférentes, lorsqu'il est effectué dans le cadre des usages professionnels licites, afin de fournir la preuve d'une transaction commerciale. Dans pareil cas, les parties aux communications doivent être informées de l'enregistrement avant qu'il n'ait lieu, de la ou des raisons pour lesquelles la communication est enregistrée et de la durée de conservation de l'enregistrement. La communication enregistrée est effacée dès que la finalité est atteinte, et en tout état de cause, lors de l'expiration du délai légal de recours contre la transaction;

(e) ne s'applique pas lorsque les moyens de communications électroniques servent à stocker des informations ou à accéder à des informations stockées dans l'équipement terminal d'un abonné, d'un utilisateur ou d'un utilisateur final moyennant utilisation de témoins de connexion («cookies») ou de dispositifs analogues à condition que ceux-ci soient utilisés à des fins légitimes et que le responsable du traitement qui les expédie ou qui permet à un tiers de les expédier fournisse à l'abonné, l'utilisateur

ou l'utilisateur final des informations claires, précises et complètes au sens de l'article 26 la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel dont sur la ou les finalité(s) du traitement en question nonobstant le droit de ce dernier de s'opposer gratuitement, sans indication de motif et à tout moment à un tel traitement.

Cette disposition ne fait pas obstacle à un stockage ou un accès techniques visant exclusivement à effectuer ou à faciliter la transmission d'une communication par la voie d'un réseau de communications électroniques, ou strictement nécessaires à la fourniture d'un service de la société de l'information expressément demandé par l'abonné, l'utilisateur ou l'utilisateur final.

(4) Quiconque contrevient aux dispositions du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 5.– Données relatives au trafic

(1) (a) Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, et dans le seul but de permettre, en tant que de besoin, la mise à disposition des autorités judiciaires d'informations, tout fournisseur de services et/ou opérateur qui traite des données relatives au trafic est tenu de conserver ces données pendant une période de 12 mois. La Commission nationale pour la protection des données peut, après consultation de l'Institut, des autorités judiciaires et des autorités compétentes en vertu des articles 88-1 à 88-4 du Code d'instruction criminelle, désigner les catégories de données non susceptibles de pouvoir servir à la recherche, à la constatation et à la poursuite des infractions pénales.

(b) Après la période de conservation prévue sub (a), le fournisseur de services et/ou l'opérateur est obligé d'effacer les données relatives au trafic concernant les abonnés, les utilisateurs et les utilisateurs finals, ou de les rendre anonymes.

(2) Tout fournisseur de services et/ou tout opérateur qui traite des données relatives au trafic concernant les abonnés, les utilisateurs et les utilisateurs finals, est tenu de prendre toutes les dispositions nécessaires à ce que de telles données soient conservées pendant la période prévue sub (1) (a) de manière telle qu'il est impossible à quiconque d'accéder à ces données dès lors qu'elles ne sont plus nécessaires à la transmission d'une communication et/ou aux traitements prévus par les dispositions sub (3) et (4), à l'exception des accès qui sont:

- ordonnées par les autorités agissant dans le cadre d'un crime flagrant ou dans le cadre de l'article 40 du Code d'instruction criminelle et celles compétentes en vertu des articles 88-1 à 88-4 du Code d'instruction criminelle conformément aux législations en vigueur pour sauvegarder la sûreté de l'Etat, la défense, la sécurité publique et pour la prévention, la recherche, la constatation et la poursuite des infractions pénales; ou
- demandées par les organes compétents conformément à la législation en vigueur dans le but de régler des litiges notamment en matière d'interconnexion ou de facturation.

jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement.

(4) Les données relatives au trafic peuvent être traitées en vue de commercialiser des services de communications électroniques ou de fournir des services à valeur ajoutée dans la mesure et pour la durée nécessaires à la fourniture ou à la commercialisation de ces services pour autant que le fournisseur d'un service de communications électroniques et/ou l'opérateur informe préalablement l'abonné, l'utilisateur ou l'utilisateur final concerné des types de données relatives au trafic traitées, de la finalité et de la durée du traitement et que celui-ci ait donné son consentement nonobstant son droit de pouvoir s'opposer à tout moment à un tel traitement.

(5) Le traitement des données relatives au trafic effectué dans le cas des activités visées aux paragraphes (1) (b); (3) et (4) est restreint aux personnes agissant sous l'autorité du fournisseur de services et/ou de l'opérateur qui sont chargées d'assurer la facturation et/ou la gestion du trafic, répondre aux demandes de clientèle, détecter les fraudes, commercialiser les services de communications électroniques ou pour fournir un service à valeur ajoutée. Le traitement doit se limiter à ce qui est nécessaire à de telles activités.

(6) Quiconque contrevient aux dispositions des paragraphes (1), (2), (4), (5) du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 6.– Facturation détaillée

(1) Tout abonné a le droit de recevoir une facture non détaillée.

(2) Les appels gratuits y compris ceux aux services d'urgence et d'alerte ne sont pas indiqués sur la facture détaillée indépendamment de son degré de détail. En outre la facture détaillée ne contient aucune indication permettant d'identifier l'appelé.

Art. 7.– Identification de la ligne appelante et de la ligne connectée

(1) Dans le cas où la présentation de l'identification de la ligne appelante est offerte en tant que service, le fournisseur du service permet à l'abonné et à l'utilisateur appelant d'empêcher, par un moyen simple et gratuit, la présentation de l'identification de la ligne appelante, et ce appel par appel. L'abonné appelant dispose de cette possibilité de manière permanente pour chaque ligne.

(2) Dans le cas où la présentation de l'identification de la ligne appelante est offerte en tant que service, l'abonné appelé doit pouvoir empêcher, par un moyen simple et gratuit pour un usage raisonnable de cette fonction, la présentation de l'identification de la ligne pour les appels entrants.

(3) Dans le cas où la présentation de l'identification de la ligne appelante est offerte en tant que service et où l'identification de la ligne appelante est présentée avant l'établissement de l'appel; l'abonné appelé doit pouvoir, par un moyen simple et gratuit, refuser les appels entrants lorsque l'utilisateur ou l'abonné appelant a empêché la présentation de l'identification de la ligne appelante.

(4) Dans le cas où la présentation de l'identification de la ligne connectée est offerte, l'abonné appelé doit pouvoir, par un moyen simple et gratuit, empêcher la présentation de l'identification de la ligne connectée auprès de la personne qui appelle.

(5) Pour les appels effectués à destination du numéro d'appel d'urgence unique européen 112 et des numéros d'urgence déterminés par l'Institut, l'identification de la ligne appelante est toujours présentée même lorsque l'appelant l'a empêché.

(6) Les dispositions du paragraphe 1^{er} s'appliquent également aux appels provenant de l'Union européenne à destination de pays tiers. Les dispositions des paragraphes (2), (3) et (4) s'appliquent également aux appels entrants provenant de pays tiers.

(7) Le fournisseur du service informe le public, par des moyens appropriés et au plus tard lors de la conclusion d'un contrat des possibilités susénoncées.

(8) L'abonné appelé prétendant être victime d'appels anonymes à contenu malveillant peut obtenir l'identification de la ligne appelante ou connectée, des appels répétés ou intempestifs, déclarés comme étant malveillants, lesquels ont été effectués ou repérés sur base d'un même numéro d'appel ou d'un même raccordement.

Un règlement grand-ducal fixera les modalités à respecter par le fournisseur du service et/ou l'opérateur ainsi que par les abonnés prétendant être victime d'appels anonymes à contenu malveillant.

Il précisera également les caractéristiques d'un appel à contenu malveillant et déterminera l'utilisation de l'identification de la ligne appelante même si sa présentation est empêchée.

(9) Quiconque contrevient aux dispositions du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 8.– Renvoi automatique d'appels

Dans le cas où le renvoi automatique d'appels (ou déviation) est offert en tant que service, le fournisseur du service confère à tout abonné la possibilité de mettre fin, par un moyen simple et gratuit, au renvoi automatique d'appels par un tiers vers son appareil terminal lorsque le fournisseur du service peut identifier l'origine des appels renvoyés. Le cas échéant, cette identification se fait en collaboration avec d'autres fournisseurs de services concernés.

Art. 9.– Données de localisation autres que les données relatives au trafic

(1) (a) Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, et dans le seul but de permettre, en tant que de besoin, la mise à disposition des autorités judiciaires d'informations, tout fournisseur de services et/ou opérateur qui traite des données de localisation autres que des données relatives au trafic est tenu de conserver ces données pendant une période de 12 mois. Pour l'application du présent paragraphe, une seule information de localisation est requise par communication ou par appel. La Commission nationale pour la protection

des données peut, après consultation de l'Institut des autorités judiciaires et des autorités compétentes en vertu des articles 88-1 à 88-4 du Code d'instruction criminelle, désigner les catégories de données non susceptibles de pouvoir servir à la recherche, à la constatation et à la poursuite des infractions pénales. Les données de localisation autres que les données relatives au trafic sont également communiquées au numéro d'appel d'urgence unique européen 112 ainsi qu'aux numéros d'urgence déterminés par l'Institut.

- (b) Après la période de conservation prévue sub (a), le fournisseur de services et/ou l'opérateur est obligé d'effacer les données de localisation autres que les données relatives au trafic concernant les abonnés, les utilisateurs et les utilisateurs finals, ou de les rendre anonymes.

(2) Tout fournisseur de services et/ou opérateur qui traite des données de localisation, autres que les données relatives au trafic, concernant les abonnés, les utilisateurs et les utilisateurs finals, est tenu de prendre toutes les dispositions nécessaires à ce que de telles données soient conservées pendant la période prévue sub (1) (a) de manière telle qu'il est impossible à quiconque d'accéder à ces données, à l'exception des accès qui sont ordonnés par les autorités agissant dans le cadre d'un crime flagrant ou dans le cadre de l'article 40 du Code d'instruction criminelle et celles compétentes en vertu des articles 88-1 à 88-4 du Code d'instruction criminelle conformément aux législations en vigueur pour sauvegarder la sûreté de l'Etat, la défense, la sécurité publique et pour la prévention, la recherche, la constatation et la poursuite des infractions pénales.

(3) Tout fournisseur de services et/ou opérateur ne peut traiter des données de localisation, autres que les données relatives au trafic, concernant les abonnés, utilisateurs et les utilisateurs finals, que si celles-ci ont été rendues anonymes ou moyennant le consentement exprès de l'abonné, de l'utilisateur ou de l'utilisateur final, dans la mesure et pour la durée nécessaire à la fourniture d'un service à valeur ajoutée sous réserve des dispositions (2), (4) et (5).

(4) Le fournisseur du service et le cas échéant l'opérateur informe préalablement l'abonné, l'utilisateur ou l'utilisateur final sur les types de données de localisation traitées, autres que les données relatives au trafic, sur la ou les finalité(s) et la durée de ce traitement ainsi que sur la transmission de ces données à des tiers en vue de la fourniture du service à valeur ajoutée et que l'abonné, l'utilisateur ou de l'utilisateur final doit avoir donné son consentement et nonobstant son droit de s'opposer gratuitement, sans indication de motif et à tout moment à un tel traitement. Dans le cas du traitement de données de localisation, autres que les données relatives au trafic, l'abonné, l'utilisateur ou l'utilisateur final doit avoir la possibilité d'interdire temporairement, par un moyen simple et gratuit, le traitement de ces données pour chaque connexion au réseau ou pour chaque transmission de communication.

(5) Le traitement effectué des données de localisation, autres que les données relatives au trafic, dans le cas des activités visées aux paragraphes (1)(b), (3) et (4) est restreint aux personnes agissant sous l'autorité du fournisseur de services et/ou de l'opérateur ou du tiers qui fournit le service à valeur ajoutée. Le traitement doit se limiter à ce qui est nécessaire à de telles activités.

(7) Quiconque contrevient aux dispositions du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 10.– Annuaire d'abonnés

(1) L'abonné, doit être informé gratuitement et au plus tard lors de la souscription de l'abonnement, des fins auxquelles sont établis des annuaires d'abonnés imprimés ou électroniques accessibles au public (ci-après «les annuaires») ou consultables par l'intermédiaire de services de renseignements, dans lesquels les données le concernant peuvent figurer, ainsi que de toute autre possibilité d'utilisation reposant sur des fonctions de recherche intégrées dans les versions électroniques des annuaires.

(2) (a) L'abonné doit avoir la possibilité d'indiquer clairement, lors de la souscription de l'abonnement ou à tout autre moment lors de nouvelles éditions de mises à jour ou d'annuaires, si les données à caractère personnel le concernant, et lesquelles de ces données doivent figurer dans un annuaire public, dans la mesure où ces données sont pertinentes par rapport à la fonction de l'annuaire en question telle qu'elle a été établie par le fournisseur de l'annuaire.

(b) L'abonné doit pouvoir vérifier, corriger ou supprimer ces données. La non-inscription dans un annuaire public d'abonnés, la vérification, la correction ou la suppression de données à caractère personnel dans un tel annuaire est gratuite.

(3) Le traitement de données à des fins d'annuaire autres que la simple recherche des coordonnées d'un abonné sur la base de son nom et, au besoin, d'un nombre limité d'autres paramètres n'est possible que si

l'abonné a donné son consentement préalable nonobstant son droit de s'opposer gratuitement, sans indication de motif et à tout moment à un tel traitement.

(4) Le présent article s'applique aux personnes physiques ainsi qu'aux personnes morales dans le respect de leurs intérêts légalement protégés.

(5) Quiconque contrevient aux dispositions du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 11.– Communications non sollicitées

(1) L'utilisation de systèmes automatisés d'appel sans intervention humaine (automates d'appel), de télécopieurs ou de courrier électronique à des fins de prospection directe n'est possible que si l'abonné a donné son consentement préalable.

(2) Sans préjudice du paragraphe (1^{er}) le fournisseur, qui dans le cadre d'une vente d'un produit ou d'un service, a obtenu directement de son client les coordonnées électroniques de celui-ci en vue d'un courrier électronique, peut exploiter ces coordonnées à des fins de prospection directe pour offrir des produits ou services analogues que lui-même fournit pour autant que ledit client soit clairement informé sur l'exploitation de ses coordonnées et nonobstant son droit de s'opposer par un moyen simple et gratuit à une telle exploitation au moment de la collecte de ses coordonnées et lors de chaque message, au cas où le client n'aurait pas d'emblée refusé une telle exploitation.

(3) L'envoi de communications non sollicitées à des fins de prospection directe par d'autres moyens que ceux visés aux paragraphes (1) et (2) n'est possible que si l'abonné concerné a donné son consentement préalable.

(4) Il est interdit d'émettre des messages électroniques à des fins de prospection directe en déguisant, dissimulant ou en dénaturant l'identité de l'émetteur au nom duquel la communication est faite, ou sans indication d'adresse valable à laquelle le destinataire peut transmettre une demande de cesser ces communications.

(5) Le présent article s'applique aux personnes physiques et aux personnes morales dans le respect de leurs intérêts légalement protégés.

(6) Quiconque contrevient aux dispositions du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 12.– Dispositions transitoires et finales

(1) La Commission nationale pour la protection des données est chargée du respect des dispositions de la présente loi dans le cadre de ses missions et pouvoirs qui lui sont attribués en vertu de l'article 32 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

(2) Le fournisseur offrant un annuaire «de recherche inverse» au sens de l'article 10 paragraphe (3) avant l'entrée en vigueur de la présente loi informe l'abonné, par un moyen approprié et gratuit, de la finalité du traitement de ses données. L'abonné qui ne s'y oppose pas dans un délai de 2 mois est censé avoir consenti à ce que ses données soient traitées à des fins de recherche inverse.

(3) *Les articles suivants du code d'instruction criminelle sont modifiés comme suit:*

(a) **Art. 88-2:** *Les alinéas 1, 2, 3 et 5 de l'article 88-2 du Code d'Instruction criminelle sont modifiés comme suit:*

al 1^{er}: Les décisions par lesquelles le juge d'instruction ou le président de la chambre du conseil de la Cour d'appel auront ordonné la surveillance et le contrôle de télécommunications ainsi que de correspondances confiées à la poste seront notifiées aux opérateurs des postes ou télécommunications qui feront sans retard procéder à leur exécution.

al 2: Ces décisions et les suites qui leur auront été données seront inscrites sur un registre spécial tenu par chaque opérateur des postes ou télécommunications.

al 3: Les télécommunications enregistrées et les correspondances ainsi que les données ou renseignements obtenus par d'autres moyens techniques de surveillance et de contrôle sur la base de l'article 88-1 seront remis sous scellés et contre récépissé au juge d'instruction qui dressera procès-verbal de leur remise. Il fera copier les correspondances pouvant servir à conviction ou à décharge

et versera ces copies, les enregistrements ainsi que tous autres données et renseignements reçus au dossier. Il renverra les écrits qu'il ne juge pas nécessaire de saisir aux opérateurs des postes qui les remettront sans délai au destinataire.

al 5: Les communications avec des personnes liées par le secret professionnel au sens de l'article 458 du code pénal et non suspectes d'avoir elles-mêmes commis l'infraction ou d'y avoir participé ne pourront être utilisées. Leur enregistrement et leur transcription seront immédiatement détruits par le juge d'instruction.

(b) **Art 88-4:** *Les alinéas 1 et 4 de l'article 88-4 sont modifiés comme suit.*

al 1^{er}: Les décisions par lesquelles le Président du Gouvernement aura ordonné la surveillance et le contrôle de télécommunications ainsi que de correspondances seront notifiées aux opérateurs des postes ou télécommunications qui feront procéder sans retard à leur exécution.

al 4: Les correspondances seront remises sous scellés et contre récépissé au service de renseignements. Le chef du service fera photocopier les correspondances pouvant servir à charge ou à décharge et renverra les écrits qu'il ne juge pas nécessaire de retenir aux opérateurs des postes qui les feront remettre au destinataire.

(4) *La loi du 2 août 2002 relative à la protection de la personne à l'égard du traitement des données à caractère personnel est modifiée comme suit:*

«Art. 3.– Champ d'application

(5) La présente loi ne s'applique pas:

- au traitement de données concernant une personne morale et dont la publication au Mémorial est prescrite par une loi ou un règlement grand-ducal.

Art. 11.– Traitement à des fins de surveillance sur le lieu du travail

(1) Le traitement à des fins de surveillance sur le lieu de travail peut être mis en oeuvre, conformément à l'article 14, par l'employeur s'il en est le responsable. Un tel traitement n'est possible que s'il est nécessaire:

- (a) pour les besoins de sécurité et de santé des travailleurs, ou
- (b) pour les besoins de protection des biens quelque soit le statut, public ou privé, de l'employeur, ou
- (c) pour le contrôle du processus de production portant uniquement sur les machines, ou
- (d) pour le contrôle temporaire de production ou des prestations du travailleur, lorsqu'une telle mesure est le seul moyen pour déterminer la rémunération exacte, ou
- (e) dans le cadre d'une organisation de travail selon l'horaire mobile conformément à la loi.
- (f) pour assurer la prévention, la recherche et la détection d'actes susceptibles d'engager la responsabilité de l'employeur quelque soit son statut, public ou privé, de l'Etat ou des collectivités publiques.

Art. 12.– Notification préalable à la Commission nationale

(2) Pour les traitements des données dont la mise en oeuvre n'est pas susceptible de porter atteinte aux libertés et droits fondamentaux, et notamment à la vie privée des personnes concernées, la Commission nationale établit et publie des directives en vue d'une notification simplifiée. Ces directives précisent:

- a) la ou les finalités du traitement faisant l'objet d'une notification simplifiée;
- b) la ou les catégories de données traitées;
- c) la ou les catégories de personnes concernées;
- d) les destinataires ou catégories de destinataires auxquels les données sont communiquées;
- e) la durée de conservation.

En dehors de ces directives, la notification simplifiée comprend les informations prévues aux points (a) et (b) de l'article 13 paragraphe (1).

Les traitements qui correspondent à ces directives font l'objet d'une notification simplifiée de conformité envoyée à la Commission nationale par support papier accompagné, le cas échéant, d'un support informatique ou d'une transmission par voie électronique.

(3) Est exempté de l'obligation de notification:

- (b) le traitement ayant pour seul objet la tenue d'un registre qui en vertu d'une loi ou d'un règlement grand-ducal est destiné à l'information du public et qui est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime;

Art. 13.– Contenu et forme de la notification

- (3) La notification se fait auprès de la Commission nationale moyennant support papier accompagné, le cas échéant, d'un support informatique ou d'une transmission par voie électronique suivant un schéma à établir par elle. Il est accusé réception de la notification.

Art. 14.– Autorisation préalable de la Commission nationale

Nouveau paragraphe (3): «Toute modification affectant les informations visées au paragraphe (2) doit être autorisée par la Commission nationale préalablement à la mise en œuvre du traitement.» *L'actuel paragraphe (3) devient le paragraphe (4). Le texte reste inchangé.*

Nouveau paragraphe (5): «Un règlement grand-ducal fixera le montant et les modalités de paiement d'une redevance à percevoir lors de toute autorisation et de toute modification d'autorisation.»

Nouveau paragraphe (6): «L'autorisation se fait auprès de la Commission nationale moyennant support papier accompagné, le cas échéant, d'un support informatique ou d'une transmission par voie électronique. Il est accusé réception de l'autorisation.» *L'actuel paragraphe (4) devient le paragraphe (7). Le texte reste inchangé.*

Art. 15.– Publicité des traitements

- (2) Figurent dans ce registre:

(a) les traitements notifiés à la Commission nationale en vertu de l'article 12, paragraphes (1) et (2)

Art. 27.– Exceptions au droit à l'information de la personne concernée

- (1) L'article 26 paragraphes (1) et (2) ne s'applique pas lorsque le traitement est nécessaire pour sauvegarder:

(g) une mission de contrôle, d'inspection ou de réglementation relevant, même à titre occasionnel, de l'exercice de l'autorité publique, dans les cas visés aux points (c), (d) et (e)

Art. 34.– Composition de la Commission nationale

En cas de cessation du mandat, il est réintégré sur sa demande dans son administration d'origine à un emploi correspondant au traitement qu'il a touché précédemment, augmenté des échelons et majorations de l'indice se rapportant aux années de service passées comme président ou membre effectif jusqu'à concurrence du dernier échelon du grade. (alinéa 6) Toutefois, si l'autorité investie du pouvoir de nomination estime que la nature du travail accompli et l'expérience acquise par l'intéressé au sein de la Commission nationale justifient sa nomination à une fonction supérieure à celle visée ci-dessus, elle peut procéder à une telle nomination sans que le bénéficiaire ne puisse, de ce fait, accéder à une fonction ou obtenir un rang plus élevé que les fonctionnaires de la même carrière entrés au service de l'Etat en même temps que lui ou avant lui (nouvel alinéa 7) A défaut de vacance, il peut être créé un emploi hors cadre correspondant à ce traitement; cet emploi est supprimé de plein droit à la première vacance qui se produit dans une fonction appropriée du cadre normal. (l'alinéa 7 devient l'alinéa 8)

Art. 41.– Dispositions spécifiques

- (1) dernier alinéa: La centrale des secours d'urgence 112, les centres d'appels d'urgence de la police grand-ducale et la centrale du service d'incendie et de sauvetage de la Ville de Luxembourg accèdent dans les mêmes conditions et modalités que les autorités visées à l'alinéa précédent aux seules données concernant l'identité des abonnés et utilisateurs des opérateurs et fournisseurs de communications électroniques.

- (3) L'accès de plein droit se limite aux mesures spéciales de surveillance telles que prévues aux articles 88-1 à 88-4 du Code d'instruction criminelle, celles prises en matière de crime flagrant ou dans le cadre de l'article 40 du Code d'instruction criminelle et aux mesures particulières de secours d'urgence dans le cadre des activités de la centrale des secours d'urgence 112, des centres d'appels d'urgence de la police grand-ducale et de la centrale du service d'incendie et de sauvetage de la Ville de Luxembourg.

Art. 13.– Entrée en vigueur

La présente loi entre en vigueur le premier jour du mois qui suit sa publication au Mémorial.

EXPOSE DES MOTIFS ET COMMENTAIRE DES ARTICLES

• *Historique*

Les nouvelles technologies numériques avancées posent actuellement des exigences spécifiques à la protection de la vie privée des utilisateurs ainsi qu'au traitement de leurs données à caractère personnel. Le développement de la société de l'information se caractérise notamment par la mise en œuvre de nouveaux services de communications électroniques. L'Internet offre certes de nouvelles possibilités aux utilisateurs mais présente également de nouveaux dangers aux utilisateurs en ce qui concerne leurs données à caractère personnel et leur vie privée. L'accès aux réseaux mobiles numériques est ouvert à un large public à des conditions de plus en plus abordables. Ces réseaux numériques offrent de grandes capacités et de vastes possibilités pour le traitement des données à caractère personnel. Le succès du développement transfrontalier des services de communications dépendra donc en grande partie de la certitude qu'auront les utilisateurs que ces services ne porteront pas atteinte à leur vie privée.

Conscients de ces dangers le Conseil, dans sa résolution du 18 juillet 1989, ainsi que le Parlement européen avaient souligné l'importance de la protection des données à caractère personnel et de la vie privée eu égard notamment à l'introduction des réseaux numériques à intégration de services (RNIS).

Des dispositions adéquates furent ainsi adoptées dans la *directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications (JOCE No L 281/31 du 23.11.1995)*.

• *But et objectifs de la Directive 97/66/CE*

La directive 97/66/CE a pour but d'harmoniser les dispositions nationales de «protection des données» afin d'éviter de créer des obstacles au marché intérieur des télécommunications conformément à l'objectif énoncé à l'article 7A du traité (considérant 8 de la directive). Elle tend à traduire les principes définis dans la directive 95/46/CE (transposée en droit national par la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel) en règles spécifiques applicables au secteur des télécommunications en renforçant d'une part la confidentialité des communications; principe garanti en conformité des instruments internationaux relatifs aux droits de l'homme dont notamment la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et les constitutions des Etats membres et d'autre part les dispositions relatives au stockage et au traitement automatisés de données relatives aux abonnés et aux utilisateurs.

De ce fait la directive 97/66/CE est une réglementation sectorielle eu égard à la réglementation générale qu'est la directive 95/46/CE. De sorte que dans le secteur des télécommunications voire des communications électroniques la directive 95/46/CE est applicable à tous les aspects de la protection des droits et libertés fondamentaux qui n'entrent pas expressément dans le cadre de la directive 97/66/CE.

• *La directive 2002/58 du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques dénommée directive «vie privée et communications électroniques».*

Afin de tenir compte de l'évolution des marchés et des technologies des services de communications électroniques, la directive 2002/58/CE est destinée à remplacer la directive 97/66/CE. La directive «vie privée et communications électroniques» ne vise pas à modifier profondément le contenu de la directive actuellement en vigueur, mais à adapter et à actualiser ses dispositions pour tenir compte des évolutions récentes et prévisibles dans le domaine des services et des technologies des communications électroniques. De ce fait elle reprend les principes de base de la directive existante moyennant des modifications rédactionnelles et l'ajout de dispositions nouvelles plus adaptées à l'environnement actuel.

Son but consiste entre autres à adopter, conformément au cadre réglementaire posé, des règles qui sont neutres sur le plan technologique c'est-à-dire des règles qui n'imposent ni ne favorisent l'utilisation d'un type de technologie particulier ce qui implique que le consommateur voire l'utilisateur jouit d'un même niveau de protection quelle que soit la technologie mise en œuvre pour la fourniture d'un service donné.

• *Etat de transposition au Luxembourg*

Vu le vide juridique total en la matière dû au retard qu'a pris le Luxembourg dans la transposition de la directive 97/66/CE (cf. arrêt de la Cour du 6 mars 2003 condamnant le le Grand-Duché de Luxembourg pour non-transposition de la directive 97/66/CE) et compte tenu de l'adoption de la directive «vie privée et communications électroniques», le présent projet de loi se propose donc de transposer à la fois les principes de base de la directive 97/66/CE (incorporés dans la directive 2002/58/CE) et les dispositions nouvelles de la directive «vie privée et communications électroniques». Pourquoi l'avoir fait maintenant et non pas lors du dépôt du projet de loi No 4735? La réponse est simple puisqu'il fallait attendre à ce que le texte communautaire

se stabilise, suite à des discussions souvent difficiles au niveau communautaire aux sujets tels que la durée de conservation des données et les communications non sollicitées qui a suscité de vives discussions quant au choix du régime de l'opt in et de l'opt out.

Commentaire des articles

Art. 1^{er}. – Champ d'application

L'article 1^{er} paragraphe (1^{er}) précise que les dispositions de la présente loi sont des dispositions spécifiques de «protection des données» applicables en matière de communications électroniques accessibles au public. En dehors du champ d'application de la présente loi, les dispositions générales de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel s'appliquent.

La présente loi s'applique donc à la fourniture de services de communications électroniques accessibles au public sur les réseaux de communications électroniques publics.

L'article 1^{er} reprend l'article 3 de la directive 97/66 dont le texte a été actualisé par la directive «vie privée et communications électroniques» qui remplace les «services de télécommunications» par ceux de «services de communications électroniques» et qui supprime la référence au RNIS et aux réseaux numériques mobiles par souci de neutralité technologique.

La référence à la «future» législation sur les réseaux et les services de communications électroniques (paragraphe 1^{er}) s'explique par le fait que la directive 2002/58/CE a initialement fait partie des directives du «paquet réglementaire des communications électroniques»¹ dont elle emprunte les concepts de base.

Art. 2. – Définitions

La directive «vie privée et communications électroniques» a remplacé les définitions existantes des «services et réseaux de télécommunications» figurant dans la directive 97/66 par celles de «services et réseaux de communications électroniques» afin d'aligner la terminologie sur la directive 2002/21/CE relative à un cadre réglementaire commun pour les réseaux et les services de communications électroniques (ci-après directive «cadre»). Une actualisation de ces définitions s'imposait pour faire en sorte que les différents types de services de communications électroniques soient couverts indépendamment de la technologie utilisée. Il résulte de l'article 2 de la directive 97/66/CE ainsi que du texte de la directive «vie privée et communications électroniques» (article 2) que les 2 textes sont complémentaires à la directive 96/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (loi du 2 août 2002 précitée) et à la directive «cadre» (mentionnée ci-dessus) de sorte que leurs définitions s'appliquent également.

L'article 2 a suivi cette démarche en reprenant les termes «appel»; «communication»; «données relatives au trafic»; «données de localisation»; «consentement»; «service à valeur ajoutée» et «courrier électronique» figurant dans le texte de la directive 2002/58/CE mais également ceux de «service de communications électroniques», «réseau de communications électroniques», «réseau de communication public» et d'«utilisateur final» figurant dans la directive «cadre» transposés en droit national par le projet de loi sur les réseaux et les services de communications électroniques. L'article 2 (a) reprend, par souci de clarté, la définition de l'«abonné» telle que prévue par la directive 97/66CE, en l'adaptant à celle figurant dans le projet de loi sur les réseaux et les services de communications électroniques. La définition de l'abonné constitue une notion clé dans le corps du texte et se caractérise par la relation contractuelle entre l'abonné (personne physique ou morale) et l'entreprise offrant des services de communications électroniques accessibles au public laquelle peut prévoir un paiement périodique ou un versement unique pour le service fourni ou à fournir; les cartes de prépaiement constituent également un contrat. Alors que l'article 2 (l) définit le terme «*utilisateur*» par opposition à celui «d'abonné» comme étant une personne qui utilise ou qui demande un service sans être «nécessairement abonnée à ce service». L'inclusion des définitions «utilisateur final» (correspond à la définition (p)) de la directive 2002/21 «directive-cadre» et «utilisateur» a pour objet, eu égard à la législation sur les réseaux et les services de communications électroniques, de citer les catégories d'utilisateurs pouvant être affectés par les dispositions du présent projet de loi.

La définition (b) relative à «*l'appel*» n'apporte pas de commentaire particulier. La définition (c) relative au «*consentement*» est calquée sur celle de la loi du 2 août 2002 (article 2 (c)).

¹ Directive 2002/19/CE «accès»
Directive 2002/20/CE «autorisation»
Directive 2002/21/CE «cadre»
Directive 2002/22/CE «Service universel»

Il résulte du nouveau considérant 16 relatif à la définition de «*communication*» (article 2 (d) du texte et article 2 (d) de la directive 2002/58/CE) que les informations diffusées par un service de radiodiffusion sur un réseau de communications public le sont à l'intention d'un nombre virtuellement illimité d'auditeurs/télespectateurs et ne constituent pas une communication au sens de la directive. Par contre, lorsqu'il est possible d'identifier l'abonné ou utilisateur individuel qui reçoit ces informations, comme, par exemple, dans le cas de la fourniture de services vidéo à la demande, les informations acheminées s'inscrivent dans la définition de «communication». Le «*courrier électronique*» (article 2 (e)) non prévu par la directive 97/66/CE, figure cependant dans le texte de la directive «vie privée et communications électroniques» (article 2 (h)) afin de tenir compte de la diversité actuelle des services de communications électroniques. Cette définition vise avant tout les «e-mails».

Les «*données relatives au trafic*» (article 2 (f)) sont définies comme «toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation». Il s'agit d'une nouvelle définition prévue par le texte de la directive 2002/58/CE permettant de poser le principe fondamental selon lequel toutes les données relatives au trafic générées durant une communication, qu'elles soient nécessaires ou non à l'établissement de la communication doivent être effacées ou rendues anonymes dès lors qu'elles ne sont plus nécessaires à la transmission d'une communication. Cette définition inclut les données de localisation générées durant l'exécution d'une communication et comprend également les «données de navigation» comme par exemple les URL/ Unique Resource Locator. Il résulte du nouveau considérant 15 du texte de la directive 2002/58/CE qu'«une communication peut inclure toute information consistant en une dénomination, un nombre ou une adresse, fournie par celui qui envoie la communication ou celui qui utilise une connexion pour effectuer la communication. Les données relatives au trafic peuvent inclure toute traduction de telles informations effectuée par le réseau par lequel la communication est transmise en vue d'effectuer la transmission. Les données relatives au trafic peuvent, entre autres, comporter des données concernant le routage, la durée, le moment ou le volume d'une communication, le protocole de référence, l'emplacement des équipements terminaux de l'expéditeur ou du destinataire, le réseau de départ ou d'arrivée de la communication, ou encore le début, la fin ou la durée d'une connexion; elles peuvent également représenter le format dans lequel la communication a été acheminée par le réseau».

Le moment exact où s'achève la transmission d'une communication, au-delà duquel les données relatives au trafic doivent être effacées sauf à des fins de facturation, peut dépendre du type de service de communications électroniques fourni. Ainsi, dans le cas d'un appel par téléphonie vocale, la transmission cesse dès que l'un ou l'autre des usagers interrompt la connexion et, dans le cas d'un courrier électronique, la transmission prend fin dès que le destinataire prend connaissance du message, généralement à partir du serveur de son fournisseur de service. Par «*données de localisation*» (article 2 (g) du texte et article 2 (c) de la directive 2002/58/CE) on entend la latitude, la longitude et l'altitude du lieu où est installé l'équipement terminal de l'utilisateur, la direction de l'acheminement, le degré de précision quant aux informations sur la localisation, l'identification de la cellule du réseau où se situe, à un moment donné, l'équipement terminal, ou encore le moment auquel l'information sur la localisation a été enregistrée.

La définition relative au «*service à valeur ajoutée*» (article 2 (k)) vise par exemple les conseils sur les forfaits tarifaires les plus avantageux ou sur le guidage routier, des informations sur l'état de la circulation, des prévisions météorologiques ou des informations touristiques etc. Les définitions relatives aux «*réseau de communications électroniques*»; «*réseau de communications public*», «*service de communications électroniques*» et à «l'utilisateur final» ont été reprises de la directive 2002/21/CE du PE et du Conseil relative à un cadre réglementaire commun pour les réseaux et les services de communications électroniques («directive-cadre»); laquelle est transposée par le projet de loi sur les réseaux et les services de communications électroniques.. Elles sont complémentaires par rapport aux définitions de la présente loi et feront l'objet d'un commentaire détaillé au projet de loi précité. En outre les dénominations «opérateur» et «fournisseur de services» ont pour objet une lecture plus facile du texte.

Article 3.– Sécurité

L'article 3 reprend le texte de l'article 4 de la directive 97/66/CE tout en remplaçant «services et réseaux de télécommunications» par «services et réseaux de communications électroniques accessibles au public». La sécurité étant un élément primordial pour le fonctionnement des réseaux et la prestation des services de communications électroniques d'où l'article 3 retient en quelque sorte une responsabilité en cascade en précisant que la responsabilité repose «primairement» sur le fournisseur de services (alinéa 1^{er}) vis-à-vis de son client et celle-ci est le cas échéant partagée conjointement avec l'opérateur lorsque la sécurité du réseau est en cause. Le fournisseur de services et le cas échéant l'opérateur sont obligés à informer les abonnés des risques particuliers liés à une atteinte à la sécurité du réseau et/ou des services (alinéa 2). Il s'agit d'une obligation de moyens qui incombe.

De tels risques peuvent notamment toucher les services de communications électroniques fournis par l'intermédiaire d'un réseau ouvert de sorte qu'il appartient au fournisseur qui offre des services de communications électroniques accessibles au public sur Internet, d'informer les abonnés des mesures qu'il envisage de prendre pour sécuriser les communications, en recourant par exemple à des types spécifiques de logiciels ou de techniques de cryptage. En revanche l'obligation d'information prévue à l'article 3 alinéa 2 ne dispense pas le fournisseur de services et le cas échéant l'opérateur en ce qui concerne la sécurité de son réseau, de prendre immédiatement les mesures appropriées pour remédier à l'atteinte ou au risque d'atteinte grave à la sécurité du réseau et de rétablir le niveau normal de sécurité du service; les frais étant à sa seule charge. Notons que l'information de l'abonné sur les risques en matière de sécurité devrait être gratuite, exceptés les frais nominaux qu'un abonné peut être amené à supporter lorsqu'il reçoit ou collecte des informations (ex. téléchargement d'un message reçu par courrier électronique).

Article 4.– Confidentialité des communications

L'article 4 pose le principe fondamental de la confidentialité des communications telle qu'énoncée à l'article 5 des directives 97/66/CE et 2002/58/CE. L'article 4 est une transposition «fidèle» de l'article 5 de la directive 2002/58/CE «directive vie privée et communications électroniques» du moins en ce qui concerne les paragraphes (1^{er}), (2), (3) a), d) et e). Les paragraphes (1^{er}) et (2) ont pour objet de préciser la responsabilité de l'opérateur. Le paragraphe 1^{er} transpose en droit national le paragraphe 1^{er} de l'article 5 de la directive 2002/58/CE en établissant en termes généraux l'obligation de confidentialité dans le chef de l'opérateur et/ou des fournisseurs de services.

Le paragraphe 2 pose le principe des interdictions ayant trait à la violation de la confidentialité des communications.

Notons que l'inobservation des paragraphes (1^{er}) et (2) est soumise à la même sanction (paragraphe 4). Le texte suit ainsi la logique de la loi du 2 août 2002 qui sanctionne les traitements illégaux sans distinguer selon l'existence ou non d'une intention dolosive.

Reste la question de l'interdiction du tiers d'intercepter des données, de les stocker, de les détenir etc.; non expressément prévue par le texte de la directive. Une telle interdiction pourrait néanmoins être retenue et faire l'objet d'une sanction à inclure aux actuels articles 509-1 et suivants du Code pénal. Le paragraphe 3 lettre (a) transpose la 2^e exception de l'article 5 paragraphe 1^{er} de la directive 2002/58/CE et n'apporte pas de commentaire particulier. En revanche le paragraphe 3 lettre (b) est une mesure nationale qui a pour objet de déterminer les autorités légalement autorisées à déroger au principe de la confidentialité. La lettre (b) reprend la systématique de l'article 41 de la loi du 2 août 2002 afin d'établir une certaine cohérence entre les deux dispositions. La lettre (b) du paragraphe 3 est une disposition générale qui permet aux autorités légales de conserver a priori toutes les données du fait qu'il leur est impossible de déterminer à l'avance pour quelle finalité exacte ces données seront conservées. En revanche la loi du 21 novembre 2002 réglementant le repérage de télécommunications et portant modification du Code d'Instruction criminelle (article 67-1 Cic) énonce les conditions dans lesquelles le recours au repérage de télécommunications est possible. Si ces conditions sont remplies, les données conservées par application de l'article 4 paragraphe 3 lettre (b) de la présente loi peuvent être utilisées. La loi réglementant le repérage peut donc être considérée comme un texte spécifique par rapport à la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel et notamment au présent projet de loi.

La lettre (c) du paragraphe 3 est une mesure nationale qui constitue la base légale à un enregistrement des communications type appels d'urgence et d'alerte. Le paragraphe (3) c) énonce les cas limitatifs pour lesquels un enregistrement est permis. Vu la difficulté de regrouper voire de catégoriser la multitude de services offerts en matière d'urgence et d'alerte; il est jugé plus opportun de se limiter aux 112 et aux numéros d'urgence tels que déterminés par l'Institut dont on vise avant tout le «113» lequel n'étant pas un numéro d'appel d'urgence officiel instauré au niveau européen par une décision communautaire comme le «112». La référence au 113 étant nécessaire afin d'éviter toute limitation en matière de prestation de secours. En revanche un numéro unique national attribué au corps des sapeurs pompiers fait défaut pour l'instant faute de réglementation adéquate et de centrale commune. Un projet est actuellement élaboré par le Ministère de l'Intérieur qui prévoit que la centrale du 112 servirait également de centrale commune aux sapeurs pompiers.

Les données relatives au trafic y afférents dont les données de localisation collectées dans les cas susénoncés sont à effacer une fois le secours apporté excepté le contenu des communications dont la conservation est nécessaire en cas de problème de compréhension ou d'ambiguïté entre l'appelant et les services d'urgence. En pratique les contestations parviennent au «113» 2 à 6 mois après l'appel. C'est pourquoi le délai de 6 mois est jugé appropriée. Le paragraphe (3) lettre (d) prévoit que l'enregistrement effectué à titre de preuve d'une transaction commerciale ou de toute autre communication etc. tombe également sous le principe la confidentialité des communications. La lettre (d) reprend le texte de l'article 5(2)

de la directive 2002/58/CE. En effet il est pratique courante que des communications commerciales sont enregistrées pour servir de preuve. Cette pratique est à considérer comme usage professionnel licite, tant que les parties à la communication en sont informées avant que l'enregistrement n'ait eu lieu, de la finalité de l'enregistrement et de la durée de stockage. Les communications enregistrées devraient être effacées dès que possible et, en tout état de cause, lors de l'expiration du délai légal de recours contre la transaction. Le paragraphe 3 lettre (e) transpose le paragraphe (3) de l'article 5 de la directive 2002/58/CE. Il s'agit d'un nouveau paragraphe ne figurant pas dans la directive 97/66/CE. L'utilisation de tels dispositifs ne devrait être autorisée qu'à des fins légitimes, et en étant portée à la connaissance de l'utilisateur concerné.

Il résulte du considérant 25 du texte de la directive 2002/58/CE que les «cookies» peuvent constituer un outil légitime pour évaluer par exemple l'efficacité de la conception d'un site et de la publicité faite sur ce site, ainsi que pour contrôler l'identité des utilisateurs effectuant des transactions en ligne. Lorsque les «cookies» sont destinés à des fins légitimes et servent à faciliter la fourniture d'un service de la société de l'information, leur utilisation doit être autorisée pour autant que l'opérateur d'un site qui les expédie ou qui permet à un tiers de les expédier via son site fournisse des informations claires et précises sur la finalité du/des dispositif(s) en question. Encore faut-il que l'utilisateur puisse refuser qu'un «cookie» ou un dispositif analogue soit greffé sur son équipement terminal. Finalement l'accès au contenu d'un site spécifique peut être subordonné au fait d'accepter, en pleine connaissance de cause, l'installation d'un «cookie» ou d'un dispositif analogue à condition que celui-ci soit de nouveau utilisé à des fins légitimes.

Le paragraphe 4 sanctionne l'inobservation des dispositions du présent article. Il reprend la même sanction que celle figurant dans la loi du 2 août 2002.

Article 5.– Données relatives au trafic

L'article 5 traduit le texte actualisé de l'article 6 de la directive 2002/58/CE. L'article 5 restreint l'utilisation par le fournisseur de services et/ou opérateur des données relatives au trafic aux seules fins de transmission de communications électroniques (au lieu des seuls appels téléphoniques prévus par la directive 97/66/CE); de facturation et de fourniture de services à valeur ajoutée moyennant le consentement de l'abonné/utilisateur et ce pour une durée limitée (paragraphe 2, 3 et 4).

Cependant, pour des raisons d'ordre pénal et pour des mesures spéciales de surveillance à constater en vertu des articles 88-1 à 88-4 Code d'instruction criminelle, les données relatives au trafic sont à conserver pendant une durée de 12 mois (paragraphe 1^{er} point (a)); pour des raisons de protection des données, le fournisseur de services et/ou l'opérateur doit néanmoins tout mettre en œuvre à ce que ces données ne soient plus accessibles à d'autres fins, dès lors qu'elles ne sont plus nécessaires à la communication, à la facturation ou, le cas échéant, à la fourniture de services à valeur ajoutée (paragraphe 2).

En outre le fournisseur de services et/ou l'opérateur est tenu d'effacer voire de rendre anonymes (paragraphe 1^{er} lettre (b)) les données relatives au trafic après expiration du délai de conservation et en l'absence d'une mesure d'enquête prise dans le cadre de l'article 40 du Code d'Instruction Criminelle. Cependant le paragraphe 2 est assorti de deux exceptions reprenant les dispositions de l'article 6 paragraphe 6 de la directive 2002/58/CE. Le délai de 12 mois est considéré au niveau communautaire comme étant le délai maximum pendant lequel les données de ce type peuvent être conservées. L'article 16 de la Convention sur la cybercriminalité du 23.11.2001 (<http://conventions.coe.int/Treaty>) prévoit une durée maximum de 90 jours.

Notons que la période de 12 mois oblige chaque fournisseur de services et/ou opérateur de conserver a priori toutes les données relatives au trafic pendant une durée de 12 mois pour les raisons indiquées ci-dessus.

Quant au paragraphe 3, le groupe sur la protection des personnes à l'égard du traitement des données à caractère personnel («groupe article 29» de la directive 95/46/CE) souligne dans sa recommandation 3/99 l'absence, au niveau communautaire, d'une harmonisation de la période durant laquelle la facture peut être légalement contestée. Le «groupe article 29» recommande à la Commission européenne d'harmoniser cette période «afin de fixer une limite au stockage des données relatives au trafic pour les besoins précis de la facturation, en vue de renforcer le droit fondamental des citoyens au respect de la vie privée»; période qu'il souhaite aussi courte que possible. En l'absence d'une telle harmonisation et il y a lieu de préciser que le délai de contestation en la matière est de 10 ans au Luxembourg.

Le paragraphe 4 traite des données pouvant être traitées en vue de commercialiser des services de communications électroniques ou de fournir des services à valeur ajoutée et contient des dispositions classiques de protection des données.

Le paragraphe 5 limite l'accès aux données relatives au trafic aux personnes agissant sous l'autorité du fournisseur de services et/ou de l'opérateur pour assurer la facturation et/ou la gestion du trafic. Le paragraphe 6 prévoit les sanctions pénales en cas de non-respect du présent article. Il s'agit d'une sanction analogue à celle prévue dans la loi du 2 août 2002.

Article 6.– Facturation détaillée

L'article 6 transpose l'article 7 de la directive 97/66/CE dont le texte est inchangé par rapport à celui de la directive 2002/58/CE excepté l'ajout relatif au «renforcement du respect de la vie privée». Eu égard à l'article 51 du projet de loi sur les réseaux et les services de communications électroniques qui fixe le niveau minimum d'une facture détaillée; l'article 6 du présent projet a pour objet de conférer aux abonnés le droit à une facture non détaillée tout en prévoyant des modalités susceptibles d'assurer le respect de la vie privée eu égard à la facture détaillée. Dans ce contexte le paragraphe 2 prévoit que les appels gratuits y compris ceux aux services d'urgence et d'alerte ne sont pas indiqués sur la facture ainsi que l'identification de l'appel jugée comme non indispensable pour l'établissement d'une facture.

Article 7.– Identification de la ligne appelante et de la ligne connectée

L'article 7 transpose l'article 8 de la directive 97/66/CE dont le texte demeure identique à celui de la directive 2002/58/CE (article 8). L'article 7 offre aux abonnés et aux utilisateurs des garanties afin de protéger leur vie privée dans le cadre de l'utilisation des services d'identification des lignes appelantes et connectées.

Il résulte du considérant 34 de la directive 2002/58/CE (considérant 19 de la directive 97/66) « qu'il est nécessaire, en ce qui concerne l'identification de la ligne appelante, de protéger le droit qu'a l'auteur d'un appel d'empêcher l'indication de l'identification de la ligne à partir de laquelle l'appel est effectué, ainsi que le droit de la personne appelée de refuser les appels provenant de lignes non identifiées; qu'il est justifié, dans des cas spécifiques, d'empêcher la suppression de l'indication de l'identification de la ligne appelante; que certains abonnés, en particulier les numéros de type «SOS» et autres organisations similaires, ont intérêt à garantir l'anonymat de ceux qui les appellent; qu'il est nécessaire, en ce qui concerne l'identification de la ligne connectée, de protéger le droit et l'intérêt légitime qu'a la personne appelée d'empêcher l'indication de l'identification de la ligne à laquelle l'auteur de l'appel est effectivement connecté, en particulier dans le cas d'appels renvoyés; que les fournisseurs de services de communications électroniques accessibles au public doivent informer leurs abonnés de l'existence, sur le réseau, de l'identification des lignes appelantes et connectées, ainsi que de tous les services offerts sur la base de l'identification des lignes appelante et connectée et des possibilités offertes en matière de protection de la vie privée; que cela permettra aux abonnés de choisir en connaissance de cause, parmi les possibilités qui leur sont offertes en matière de protection de la vie privée, celles dont ils souhaiteraient faire usage; que les possibilités qui sont offertes en matière de protection de la vie privée pour chaque ligne ne doivent pas nécessairement être disponibles comme un service automatique du réseau, mais peuvent être obtenues sur simple demande auprès du fournisseur du service de communications électroniques accessible au public».

L'article 7 paragraphe (5) transpose l'article 9 b) de la directive 97/66 (article 10 b) de la directive 2002/58/CE). Il constitue une dérogation au principe énoncé aux paragraphes précédents dans la mesure où il est indispensable, dans le cadre d'une prestation efficace de sauvegarde de la vie humaine, que les numéros d'appel d'urgence tels que le 112, mais également les sapeurs pompiers professionnels et le 113 (voir commentaire article 4 (3) c)), puissent répondre aux appels d'urgence et de ce fait identifier la ligne appelante même si l'appelant s'y est opposé¹.

Les paragraphes 6 et 7 n'apportent pas de commentaire particulier.

L'article 7 paragraphe (8) transpose l'article 9 a) de la directive 97/66/CE (article 10 a) de la directive 2002/58/CE). Il tend à résoudre le phénomène des appels à contenu malveillant ou dérangeant en déterminant les conditions dans lesquelles la victime d'un appel à contenu malveillant peut obtenir l'identification de l'auteur. En revanche compte tenu des modalités techniques assez complexes à respecter par l'opérateur et/ou le fournisseur de services en la matière, un règlement grand-ducal déterminant les modalités procédurales minimum est indispensable. Notons que le paragraphe 8 n'entend point déroger à l'article 6 de la loi du 11 août 1982 – Loi concernant la protection de la vie privée – mais entend apporter des précisions quant aux aspects de «protection des données» ainsi qu'à la procédure applicable en la matière.

Le paragraphe 9 incrimine les pratiques d'identification et de communication de ces informations contraires.

Article 8.– Renvoi automatique d'appels

L'article 8 transpose l'article 10 de la directive 97/66/CE dont le texte demeure inchangé à l'article 11 du texte de la directive 2002/58/CE.

L'article 8 confère à l'abonné le droit et les moyens de mettre fin au renvoi d'appels sur leur ligne. Le but est de protéger l'abonné contre toute gêne que pourrait causer le renvoi automatique d'appels par d'autres personnes et de donner à l'abonné les moyens de faire cesser le transfert des appels renvoyés sur son terminal et ceci sur simple demande adressée au fournisseur de ce service.

¹ Voir commentaire quant aux 112 et 113 à l'article 4 §3 lettre c).

Article 9.– Données de localisation autres que les données relatives au trafic

L'article 9 transpose l'article 9 du texte de la directive 2002/58/CE. Il s'agit d'un nouveau texte ne figurant pas dans la directive 97/66/CE qui introduit des garanties de respect de la vie privée des abonnés ou utilisateurs en matière de fourniture de services d'informations fondés sur la localisation des mobiles.

Dans les réseaux de communications mobiles, les données de localisation comportant des indications sur la position géographique d'un équipement terminal de l'utilisateur mobile sont traitées afin de permettre la transmission des communications. Ces données sont des données relatives au trafic couvertes par l'article 5. Toutefois les réseaux numériques mobiles peuvent également traiter des données de localisation qui sont plus précises que ne l'exige la transmission des communications et qui sont utilisées pour la fourniture de services à valeur ajoutée tels que par exemple les services personnalisés d'informations sur la circulation et le guidage des conducteurs. Il s'agit alors de données de localisation autres que les données relatives au trafic couvertes par le présent article. Vu leur caractère sensible, le traitement en vue de la fourniture de services à valeur ajoutée n'est possible que lorsque l'abonné ou l'utilisateur a donné son consentement préalable et qu'il a été informé du type de données de localisation traitées (autres que les données relatives au trafic), de leur finalité, de la durée du traitement ainsi que de la transmission de ces données à des tiers en vue de la fourniture du service à valeur ajoutée (paragraphe 4). L'abonné ou l'utilisateur doit en outre disposer d'un moyen simple et gratuit pour interdire temporairement le traitement de ce type de données (paragraphe 4 alinéa 2). Le paragraphe 3 pose le principe de la durée du traitement. Ainsi les données de localisation autres que les données relatives au trafic ne peuvent être traitées qu'«après les avoir rendues anonymes ou moyennant le consentement exprès de l'abonné ou de l'utilisateur, dans la mesure et pour la durée nécessaire à la fourniture d'un service à valeur ajoutée».

Les paragraphes 1^{er} et 2 étant le corollaire de l'article 5 et n'apportent pas de commentaire particulier ici. Cependant l'article 9 paragraphe (1^{er}) (a) précise que pour l'application du présent paragraphe «une seule information de localisation est requise par communication ou par appel» et ceci afin de limiter le volume d'informations générées par les utilisateurs mobiles lesquels se trouvent en déplacement constant. La dernière phrase de l'article 9 paragraphe (1^{er}) (a) souligne que ces données doivent également être communiquées au numéro d'appel d'urgence unique européen 112 ainsi qu'aux numéros d'urgence déterminés par l'Institut afin de permettre la localisation d'une personne en détresse. Le paragraphe (7) prévoit la même sanction qu'à l'article 5 paragraphe (7) et n'apporte pas de commentaire particulier.

Article 10.– Annuaire d'abonnés

L'article 10 transpose l'article 12 des directives 2002/58/CE et 97/66/CE tout en supprimant la possibilité de monnayer le droit de ne pas figurer dans un annuaire; disposition conforme à l'article 45 du projet de loi sur les réseaux et les services de communications électroniques. L'article 10 tient également compte des nouveaux services de communications électroniques et des nouveaux types de services d'annuaires.

Les annuaires d'abonnés aux services de communications électroniques sont librement commercialisés et largement diffusés et publiés. Pour protéger la vie privée des personnes physiques et l'intérêt légalement protégé des personnes morales, il importe que l'abonné soit à même de déterminer si les données à caractère personnel qui le concernent doivent être publiées dans un annuaire et, dans l'affirmative, lesquelles de ces données doivent être rendues publiques (paragraphe 2). Il convient que l'opérateur et/ou le fournisseur d'annuaires publics informent les abonnés figurant dans ces annuaires des fins auxquelles ceux-ci sont établis (paragraphe 1^{er}) et de toute utilisation particulière qui peut être faite des versions électroniques des annuaires publics, notamment grâce aux fonctions de recherche intégrées dans le logiciel, telles que les fonctions de recherche inverse qui permettent aux utilisateurs d'un annuaire de trouver le nom et l'adresse d'un abonné à partir d'un numéro de téléphone. Dans ce cas, il s'agirait d'une nouvelle finalité qui ne serait pas compatible avec la finalité primaire, et de ce fait en principe illicite selon le régime général de la loi du 2 août 2002 à moins que la personne concernée n'ait expressément consenti au traitement de ses données à ces nouvelles fins (paragraphe 3). Ainsi, le consentement informé des personnes concernées à l'inclusion de leurs données dans des annuaires publics pour des recherches inversées est donc indispensable. Le paragraphe 4 précise le champ d'application du présent article. Le paragraphe 5 assortit l'inobservation du présent article d'une sanction.

Article 11.– Communications non sollicitées

L'article 11 transpose l'article 13 du texte de la directive 2002/58/CE dont les paragraphes 1^{er} (à l'exception de l'intégration du «courrier électronique» dans le système de l'opt in) et 3 demeurent inchangés par rapport à l'article 12 de la directive 97/66/CE. Le paragraphe 1^{er} intègre le courrier électronique dans le système «opt in» prévu à l'article 13 paragraphe (1^{er}) de la directive 2002/58/CE. Il résulte du texte de la directive précitée que le marché unique exige actuellement une approche harmonisée selon laquelle les communications non sollicitées à des fins de prospection directe ne peuvent être envoyées

que si l'expéditeur a obtenu le consentement préalable du destinataire («opt in»). Des discussions controversées ont eu lieu au niveau communautaire entre «l'opt out» (envoi de communications non sollicitées à moins que l'abonné ait clairement refusé) et «l'opt in» (envoi de communications non sollicitées que si l'abonné a donné son consentement préalable) et ont finalement fait pencher la balance en faveur de «l'opt in». L'article 48 de la loi sur le commerce électronique, ayant initialement retenu le système de l'«opt out» pour les communications commerciales non sollicitées; a dû être modifié en conséquence (v. projet de loi No 5095 modifiant la loi du 14 août 2000 relative au commerce électronique). Le paragraphe (2) reprend l'article 13 paragraphe (2) de la directive 2002/58/CE ne figurant pas à l'article 12 de la directive 97/66/CE. Le paragraphe (2) permet à un fournisseur qui vend des produits ou services à son client d'exploiter les coordonnées électroniques collectées auprès de celui-ci pour proposer à ce client des produits ou services analogues. Il s'agirait de ce fait de données collectées à une fin précise pouvant être réutilisées ultérieurement à cette même fin au seul profit de la personne concernée en vue de lui proposer des produits ou services analogues. Notons que le texte de l'article 48 paragraphe (3) du projet de loi modifiant la loi du 14 août 2000 relative au commerce électronique est aligné sur le texte du présent paragraphe.

Le paragraphe (3) (article 13 paragraphe 3 de la directive 2002/58/CE) soumet également à l'«opt in» l'envoi de communications non sollicitées à des fins de prospection directe par d'autres moyens que ceux visés aux paragraphes (1^{er}) et (2) tels que par exemple les appels téléphoniques personnels ou les envois de publicité adressés par voie postale. Ce choix s'explique par un niveau de protection plus adéquat de la personne concernée dans la mesure où celle-ci doit donner son consentement préalable à un tel envoi et que l'émetteur a l'obligation d'informer le destinataire avant l'envoi. En cas de doute la charge de la preuve incombe donc à l'émetteur lequel doit prouver qu'il a informé le destinataire tandis que l'«opt out» fait peser la charge de la preuve au destinataire lequel doit prouver qu'il ne souhaite pas recevoir ce type de communications respectivement qu'il figure sur un «registre d'opt out».

Tandis que l'article 48 paragraphe (3) du projet de loi modifiant la loi du 14 août 2000 relative au commerce électronique retient actuellement le système de «l'opt in» pour les seules communications commerciales non sollicitées; l'article 11 du présent projet de loi introduit le système de l'«opt in» pour l'ensemble des communications électroniques non sollicitées donc celles à caractère commercial et celles n'ayant pas de caractère commercial.

Le paragraphe (4) transpose l'article 13 paragraphe (4) de la directive 2002/58/CE non prévu à l'article 12 de la directive 97/66/CE. Le paragraphe (4) énonce le principe selon lequel il est interdit d'émettre des messages non sollicités à des fins de prospection directe sous une fausse identité, une identité déguisée ou dissimulée, une fausse adresse de réponse ou une adresse de réponse déguisée ou un faux numéro. Il s'agit d'une précision utile apportée au phénomène du «spamming». Le paragraphe (5) précise que le présent article s'applique aux personnes physiques et morales. Le paragraphe (6) ne mérite pas d'observation particulière.

Article 12.– Dispositions finales

L'article 12 paragraphe (1^{er}) précise que la Commission nationale est chargée du respect des dispositions de la présente loi. Cette mission se situe dans le cadre des missions et pouvoirs d'ordre général qui sont attribués à la commission nationale en vertu de l'article 32 de la loi du 2 août 2002. *L'article 12 paragraphe (2)* a pour objet de régulariser la situation existante à ce jour. *L'article 12 paragraphe (3)* modifie les articles 88-2 et 88-4 du Code d'instruction criminelle dont la terminologie est devenu obsolète au regard de la libéralisation des marchés des postes et télécommunications. Il s'agit de modifications purement rédactionnelles.

(a) Modification de l'article 88-2 du CIC:

Les modifications apportées aux différents alinéas de l'article 88-2 sont uniquement des adaptations d'ordre rédactionnel.

Ainsi faut-il remplacer à plusieurs endroits les termes de «directeur de l'Administration des postes et télécommunications» par ceux de «opérateurs des postes ou télécommunications».

En effet, l'Administration des Postes et télécommunications n'a plus le monopole de la diffusion des télécommunications, suite à la libéralisation du marché des télécommunications.

En ce qui concerne l'envoi de courrier, il faut noter qu'à côté des services offerts par la poste, les usagers font de plus en plus souvent appel à des prestataires de services universels indépendants (par exemple: DHL, OCS, TNT etc.).

Il faut dès lors adapter les termes employés à l'article 88-2 pour étendre le champ d'application de l'article à tous les opérateurs intervenant sur ce marché. En ce qui concerne les modifications apportées à l'alinéa 3, il faut noter que par le terme «écrits» utilisé à la dernière phrase de l'alinéa 3, les auteurs de la loi du 26 novembre 1982 visaient exclusivement la correspondance envoyée par voie postale. Il suffit dès lors de faire

référence à l'alinéa 3 aux seuls opérateurs des postes. Par ailleurs, conformément à la directive 97/66/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications et la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, il est important que les opérateurs remettent sans délai les «écrits» non retenus ou saisis au destinataire.

Enfin, à l'alinéa 5 et en ce qui concerne les personnes liées par le secret professionnel, il est proposé de faire référence à l'article 458 du code pénal, conformément à la rédaction retenue par les articles 88-1 et 88-4 alinéa 3 CIC.

(b) Modification de l'article 88-4 du CIC:

Conformément aux modifications apportées à l'article 88-2, il est proposé de remplacer les termes «Directeur de l'administration des Postes et Télécommunications» par «Opérateurs des Postes». L'article 12 paragraphe (4) apporte des modifications à la loi du 2 août 2002 en vue de redresser certaines incohérences ayant créées des difficultés quant à l'application de certaines dispositions.

Art. 3.– Champ d'application

A l'article 3 paragraphe (5) second tiret:

L'ajout de la référence au Mémorial précise que les données des personnes morales qui doivent être publiées au Mémorial en application de la loi du 10 août 1915 sur les sociétés commerciales sont exclues du champ d'application de la loi du 2 août 2002 précitée. Ceci par opposition au registre destiné à l'information et à la consultation du public lequel est exempt de notification (article 12 paragraphe (3) lettre (b)) et de publication au registre public tenu par la Commission nationale en vertu de l'article 15 paragraphe (7).

L'article 3 paragraphe (5) second tiret ajoute également au terme de «règlement» les mots «grand-ducal» par souci de cohérence avec la terminologie utilisée aux articles 12 paragraphe (3) et 15 paragraphe (7).

Art. 11. Traitement à des fins de surveillance sur le lieu du travail

Article 11 paragraphe (1^{er}) lettre (b):

Afin de remédier aux interrogations quant à l'applicabilité de l'article 11 à une entité publique, l'article 11 paragraphe (1^{er}) lettre (b) supprime la notion d'«entreprise» pour la remplacer par l'expression générale de «biens de production» permettant d'englober ceux d'une entité privée et d'une entité publique.

Article 11.– paragraphe (1^{er}) lettre (f)

L'insertion d'une lettre (f) à l'article 11 paragraphe (1^{er}) permet de tenir compte de la question de savoir si l'Etat est autorisé à effectuer un traitement à des fins de surveillance si des actes sont susceptibles d'engager sa responsabilité civile ou pénale. Cas de figure non prévu par la loi du 2 août 2002.

Art. 12.– Notification préalable à la Commission nationale

L'article 12 paragraphe (2) ajoute à la fin de l'énumération des directives une nouvelle phrase qui a pour objet d'établir une cohérence entre les indications à fournir pour une notification dite «ordinaire» (voir article 13) et celles à fournir pour une notification simplifiée (article 12 paragraphe (2)). En effet il ne va pas sans dire que la personne qui notifie doit également indiquer le nom et l'adresse du responsable du traitement et le cas échéant de son représentant ou du sous-traitant (article 13 paragraphe (1^{er}) lettre a)) ainsi que la condition de légitimité du traitement (article 13 paragraphe (1^{er}) lettre b)) qui est une condition essentielle de tout traitement de données.

La dernière phrase de l'article 12 paragraphe (2) précise que (la notification doit se faire) «par support papier accompagné, le cas échéant, d'un support informatique ou d'une transmission par voie électronique».

Suite au schéma de notification établi par la Commission nationale et en l'absence à ce stade d'un système de signature électronique opérationnel, il est jugé nécessaire de ne pas se délimiter dans la détermination de la forme de la soumission des requêtes de notification. Il s'agit avant tout d'une disposition facilitant le traitement des notifications en pratique.

L'article 12 paragraphe (3) lettre b) remplace l'expression «disposition légale» par celle «d'une loi ou d'un règlement grand-ducal». Le but étant d'aligner le texte sur celui de l'article 15 paragraphe (7).

Art. 13.– Contenu et forme de la notification

Article 13 paragraphe (3) Voir observations sous article 12 (dernière phrase de l'article 12 paragraphe (2)).

Art. 14.– Autorisation préalable de la Commission nationale

Il est inséré un *nouveau paragraphe (3)* qui détermine le sort réservé à toute modification d'une autorisation préalable. Il s'agissait d'un oubli de la part du législateur lors de l'élaboration de la loi du 2 août 2002 précitée.

L'actuel paragraphe (3) devient le paragraphe (4). Le texte reste inchangé.

Il est également inséré un nouveau paragraphe (5) qui prévoit la perception d'une redevance pour les autorisations et ceci afin d'établir un certain parallélisme entre les procédures de notification et d'autorisation préalable.

Les dispositions du *nouveau paragraphe (6)* se situent dans le contexte des modifications apportées aux articles 12 paragraphe (2) et 13 paragraphe (3). Son but étant d'aligner le texte des 3 types de procédures (notification «ordinaire», notification simplifiée, autorisation) Il s'agit également d'une disposition facilitant le traitement des autorisations en pratique.

Art. 15.– Publicité des traitements

L'article 15 paragraphe (2) lettre a) essaie de pallier à un oubli en précisant que le registre public tenu par la Commission nationale contient les notifications dites «ordinaires» (article 12 paragraphe (1^{er})) ainsi que les notifications simplifiées (article 12 paragraphe (2)).

Art. 27.– Exceptions au droit à l'information de la personne concernée

L'article 27 paragraphe (1^{er}) de la loi rajoute un point g) ayant une teneur identique à celle du point h) des articles 15 paragraphe (5) et 29 paragraphe (1^{er}). Il s'agit de redresser une omission alors que l'article 13 f) de la directive porte indistinctement sur le droit à l'information (art. 27) le droit d'accès (art. 28), et sur la publicité instaurée au moyen du registre national des traitements (art. 15).

Art. 34.– Composition de la Commission nationale

Il y a lieu d'insérer à l'article 34 paragraphe (2) second paragraphe entre les alinéas 6 et 7 un nouvel alinéa avec la teneur suivante:

«Toutefois, si l'autorité investie du pouvoir de nomination estime que la nature du travail accompli et l'expérience acquise par l'intéressé au sein de la Commission nationale justifient sa nomination à une fonction supérieure à celle visée ci-dessus, elle peut procéder à une telle nomination sans que le bénéficiaire ne puisse, de ce fait, accéder à une fonction ou obtenir un rang plus élevé que les fonctionnaires de la même carrière entrés au service de l'Etat en même temps que lui ou avant lui.» Par souci de parallélisme des textes, cette modification a pour objet de reprendre le texte figurant à l'article 8 paragraphe (1^{er}) alinéa 3 de la loi du 25 juillet 2002 dont la loi du 2 août 2002 s'est inspirée.

Art. 41.– Dispositions spécifiques

L'article 41 paragraphe (1^{er}) dernier alinéa ainsi que le paragraphe (3) ajoute au 112 et à la centrale du service d'incendie et de sauvetage de la Ville de Luxembourg également les centres d'appels d'urgence de la police grand-ducale.

Cet ajout permet de tenir compte d'une réalité existante au Luxembourg. En effet l'existence de 2 centres d'appels d'urgence à savoir le 112 et 113 est un fait et perçu comme tel dans le comportement des citoyens. La limitation du mécanisme prévu à l'article 41 au 112 et aux «pompiers de la Ville de Luxembourg» reviendrait à introduire une hiérarchie dans la prestation du secours. Notons en outre que la police grand-ducale contient 2 unités distinctes à savoir la police de secours et la police judiciaire avec 2 directions distinctes chacune. La police judiciaire est couverte par le champ d'application de l'article 41 par le biais de l'article 40 du code d'instruction criminelle; une exclusion de la police de secours de l'article 41 serait dès lors peu logique pour les raisons susénoncées.

Art. 13.– Entrée en vigueur

Sans commentaire.

Autres références.

Directive n° 1 de la Commission Nationale de Protection des Données en vue d'une notification simplifiée, délibération n° 4/2003 du 1^{er} août 2003 concernant les traitements de données à caractère personnel relatifs à la gestion des membres, des administrateurs, des volontaires, des bienfaiteurs et des sympathisants des associations ou des fondations sans but lucratif régies par la loi modifiée du 21 avril 1928 ainsi que des associations de fait:

disponible depuis <http://www.cnpd.lu>

Directive n° 2 de la Commission Nationale de Protection des Données en vue d'une notification simplifiée, délibération n° 5/2003 du 1^{er} août 2003 concernant les traitements de données à caractère personnel relatifs à l'administration du personnel et des collaborateurs externes y compris celle des rémunérations:

disponible depuis <http://www.cnpd.lu>

Directive n° 3 de la Commission Nationale de Protection des Données en vue d'une notification simplifiée, délibération n° 6/2003 du 1^{er} août 2003 concernant les traitements de données à caractère personnel relatif à l'enregistrement et à l'administration des actionnaires ou des associés:

disponible depuis <http://www.cnpd.lu>

Directive n° 4 de la Commission Nationale de Protection des Données en vue d'une notification simplifiée, délibération n° 7/2003 du 1^{er} août 2003 concernant les traitements de données à caractère personnel relatifs à la gestion des contacts et des relations publiques, sociales et professionnelles pour l'organisation:

disponible depuis <http://www.cnpd.lu>

Directive n° 5 de la Commission Nationale de Protection des Données en vue d'une notification simplifiée, délibération n° 8/2003 du 1^{er} août 2003 concernant les traitements de données à caractère personnel relatifs à l'administration des fournisseurs, la gestion des commandes émises, le paiement des fournisseurs, la prospection de fournisseurs potentiels et leur évaluation:

disponible depuis <http://www.cnpd.lu>

Directive n° 6 de la Commission Nationale de Protection des Données en vue d'une notification simplifiée, délibération n° 9/2003 du 1^{er} août 2003 concernant les traitements de données à caractère personnel relatifs à l'administration de la clientèle sur la base des achats, des transactions commerciales ou autres relations professionnelles, à l'élaboration de profils de la clientèle existante, la prospection de nouveaux clients, le marketing et la publicité personnalisée:

disponible depuis <http://www.cnpd.lu>

II - Textes communautaires

Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

(JOCE L - 281 du 23 novembre 1995, p. 31).

Le parlement européen et le conseil de l'union européenne,
vu le traité instituant la Communauté européenne, et notamment son article 100 A,
vu la proposition de la Commission¹,
vu l'avis du Comité économique et social²,
statuant conformément à la procédure visée à l'article 189 B du traité³,

(1) considérant que les objectifs de la Communauté, énoncés dans le traité, tel que modifié par le traité sur l'Union européenne, consistent à réaliser une union sans cesse plus étroite entre les peuples européens, à établir des relations plus étroites entre les Etats que la Communauté réunit, à assurer par une action commune le progrès économique et social en éliminant les barrières qui divisent l'Europe, à promouvoir l'amélioration constante des conditions de vie de ses peuples, à préserver et conforter la paix et la liberté, et à promouvoir la démocratie en se fondant sur les droits fondamentaux reconnus dans les constitutions et les lois des Etats membres, ainsi que dans la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales;

(2) considérant que les systèmes de traitement de données sont au service de l'homme; qu'ils doivent, quelle que soit la nationalité ou la résidence des personnes physiques, respecter les libertés et droits fondamentaux de ces personnes, notamment la vie privée, et contribuer au progrès économique et social, au développement des échanges ainsi qu'au bien-être des individus;

(3) considérant que l'établissement et le fonctionnement du marché intérieur dans lequel, conformément à l'article 7 A du traité, la libre circulation des marchandises, des personnes, des services et des capitaux est assurée, nécessitent non seulement que des données à caractère personnel puissent circuler librement d'un Etat membre à l'autre, mais également que les droits fondamentaux des personnes soient sauvegardés;

(4) considérant que, dans la Communauté, il est fait de plus en plus fréquemment appel au traitement de données à caractère personnel dans les divers domaines de l'activité économique et sociale; que les progrès des technologies de l'information facilitent considérablement le traitement et l'échange de ces données;

(5) considérant que l'intégration économique et sociale résultant de l'établissement et du fonctionnement du marché intérieur au sens de l'article 7 A du traité va nécessairement entraîner une augmentation sensible des flux transfrontaliers de données à caractère personnel entre tous les acteurs de la vie économique et sociale des Etats membres, que ces acteurs soient privés ou publics; que l'échange de données à caractère personnel entre des entreprises établies dans des Etats membres différents est appelé à se développer; que les administrations des Etats membres sont appelées, en application du droit communautaire, à collaborer et à échanger entre elles des données à caractère personnel afin de pouvoir accomplir leur mission ou exécuter des tâches pour le compte d'une administration d'un autre Etat membre, dans le cadre de l'espace sans frontières que constitue le marché intérieur;

(6) considérant, en outre, que le renforcement de la coopération scientifique et technique ainsi que la mise en place coordonnée de nouveaux réseaux de télécommunications dans la Communauté nécessitent et facilitent la circulation transfrontalière de données à caractère personnel;

(7) considérant que les différences entre Etats membres quant au niveau de protection des droits et libertés des personnes, notamment du droit à la vie privée, à l'égard des traitements de données à caractère

¹ JO n° C 277 du 5. 11. 1990, p. 3.

JO n° C 311 du 27. 11. 1992, p. 30.

² JO n° C 159 du 17. 6. 1991, p. 38.

³ Avis du Parlement européen du 11 mars 1992 (JO n° C 94 du 13. 4. 1992, p. 198), confirmé le 2 décembre 1993 (JO n° C 342 du 20. 12. 1993, p. 30); position commune du Conseil du 20 février 1995 (JO n° C 93 du 13. 4. 1995, p. 1) et décision du Parlement européen du 15 juin 1995 (JO n° C 166 du 3. 7. 1995).

personnel peuvent empêcher la transmission de ces données du territoire d'un Etat membre à celui d'un autre Etat membre; que ces différences peuvent dès lors constituer un obstacle à l'exercice d'une série d'activités économiques à l'échelle communautaire, fausser la concurrence et empêcher les administrations de s'acquitter des responsabilités qui leur incombent en vertu du droit communautaire; que ces différences de niveau de protection résultent de la disparité des dispositions nationales législatives, réglementaires et administratives;

(8) considérant que, pour éliminer les obstacles à la circulation des données à caractère personnel, le niveau de protection des droits et libertés des personnes à l'égard du traitement de ces données doit être équivalent dans tous les Etats membres; que cet objectif, fondamental pour le marché intérieur, ne peut pas être atteint par la seule action des Etats membres, compte tenu en particulier de l'ampleur des divergences qui existent actuellement entre les législations nationales applicables en la matière et de la nécessité de coordonner les législations des Etats membres pour que le flux transfrontalier de données à caractère personnel soit réglementé d'une manière cohérente et conforme à l'objectif du marché intérieur au sens de l'article 7 A du traité; qu'une intervention de la Communauté visant à un rapprochement des législations est donc nécessaire;

(9) considérant que, du fait de la protection équivalente résultant du rapprochement des législations nationales, les Etats membres ne pourront plus faire obstacle à la libre circulation entre eux de données à caractère personnel pour des raisons relatives à la protection des droits et libertés des personnes, notamment du droit à la vie privée; que les Etats membres disposeront d'une marge de manoeuvre qui, dans le contexte de la mise en oeuvre de la directive, pourra être utilisée par les partenaires économiques et sociaux; qu'ils pourront donc préciser, dans leur législation nationale, les conditions générales de licéité du traitement des données; que, ce faisant, les Etats membres s'efforceront d'améliorer la protection assurée actuellement par leur législation; que, dans les limites de cette marge de manoeuvre et conformément au droit communautaire, des disparités pourront se produire dans la mise en oeuvre de la directive et que cela pourra avoir des incidences sur la circulation des données tant à l'intérieur d'un Etat membre que dans la Communauté;

(10) considérant que l'objet des législations nationales relatives au traitement des données à caractère personnel est d'assurer le respect des droits et libertés fondamentaux, notamment du droit à la vie privée reconnu également dans l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et dans les principes généraux du droit communautaire; que, pour cette raison, le rapprochement de ces législations ne doit pas conduire à affaiblir la protection qu'elles assurent mais doit, au contraire, avoir pour objectif de garantir un niveau élevé de protection dans la Communauté;

(11) considérant que les principes de la protection des droits et des libertés des personnes, notamment du droit à la vie privée, contenus dans la présente directive précisent et amplifient ceux qui sont contenus dans la convention, du 28 janvier 1981, du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel;

(12) considérant que les principes de la protection doivent s'appliquer à tout traitement de données à caractère personnel dès lors que les activités du responsable du traitement relèvent du champ d'application du droit communautaire; que doit être exclu le traitement de données effectué par une personne physique dans l'exercice d'activités exclusivement personnelles ou domestiques, telles la correspondance et la tenue de répertoires d'adresses;

(13) considérant que les activités visées aux titres V et VI du traité sur l'Union européenne concernant la sécurité publique, la défense, la sûreté de l'Etat ou les activités de l'Etat dans le domaine pénal ne relèvent pas du champ d'application du droit communautaire, sans préjudice des obligations incombant aux Etats membres au titre de l'article 56 paragraphe 2 et des articles 57 et 100 A du traité; que le traitement de données à caractère personnel qui est nécessaire à la sauvegarde du bien-être économique de l'Etat ne relève pas de la présente directive lorsque ce traitement est lié à des questions de sûreté de l'Etat;

(14) considérant que, compte tenu de l'importance du développement en cours, dans le cadre de la société de l'information, des techniques pour capter, transmettre, manipuler, enregistrer, conserver ou communiquer les données constituées par des sons et des images, relatives aux personnes physiques, la présente directive est appelée à s'appliquer aux traitements portant sur ces données;

(15) considérant que les traitements portant sur de telles données ne sont couverts par la présente directive que s'ils sont automatisés ou si les données sur lesquelles ils portent sont contenues ou sont destinées à être contenues dans un fichier structuré selon des critères spécifiques relatifs aux personnes, afin de permettre un accès aisé aux données à caractère personnel en cause;

(16) considérant que les traitements des données constituées par des sons et des images, tels que ceux de vidéo-surveillance, ne relèvent pas du champ d'application de la présente directive s'ils sont mis en

oeuvre à des fins de sécurité publique, de défense, de sûreté de l'Etat ou pour l'exercice des activités de l'Etat relatives à des domaines du droit pénal ou pour l'exercice d'autres activités qui ne relèvent pas du champ d'application du droit communautaire;

(17) considérant que, pour ce qui est des traitements de sons et d'images mis en oeuvre à des fins de journalisme ou d'expression littéraire ou artistique, notamment dans le domaine audiovisuel, les principes de la directive s'appliquent d'une manière restreinte selon les dispositions prévues à l'article 9;

(18) considérant qu'il est nécessaire, afin d'éviter qu'une personne soit exclue de la protection qui lui est garantie en vertu de la présente directive, que tout traitement de données à caractère personnel effectué dans la Communauté respecte la législation de l'un des Etats membres; que, à cet égard, il est opportun de soumettre les traitements de données effectués par toute personne opérant sous l'autorité du responsable du traitement établi dans un Etat membre à l'application de la législation de cet Etat;

(19) considérant que l'établissement sur le territoire d'un Etat membre suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable; que la forme juridique retenue pour un tel établissement, qu'il s'agisse d'une simple succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à cet égard; que, lorsqu'un même responsable est établi sur le territoire de plusieurs Etats membres, en particulier par le biais d'une filiale, il doit s'assurer, notamment en vue d'éviter tout contournement, que chacun des établissements remplit les obligations prévues par le droit national applicable aux activités de chacun d'eux;

(20) considérant que l'établissement, dans un pays tiers, du responsable du traitement de données ne doit pas faire obstacle à la protection des personnes prévue par la présente directive; que, dans ce cas, il convient de soumettre les traitements de données effectués à la loi de l'Etat membre dans lequel des moyens utilisés pour le traitement de données en cause sont localisés et de prendre des garanties pour que les droits et obligations prévus par la présente directive soient effectivement respectés;

(21) considérant que la présente directive ne préjuge pas des règles de territorialité applicables en matière de droit pénal;

(22) considérant que les Etats membres préciseront dans leur législation ou lors de la mise en oeuvre des dispositions prises en application de la présente directive les conditions générales dans lesquelles le traitement de données est licite; que, en particulier, l'article 5, en liaison avec les articles 7 et 8, permet aux Etats membres de prévoir, indépendamment des règles générales, des conditions particulières pour les traitements de données dans des secteurs spécifiques et pour les différentes catégories de données visées à l'article 8;

(23) considérant que les Etats membres sont habilités à assurer la mise en oeuvre de la protection des personnes, tant par une loi générale relative à la protection des personnes à l'égard du traitement des données à caractère personnel que par des lois sectorielles telles que celles relatives par exemple aux instituts de statistiques;

(24) considérant que les législations relatives à la protection des personnes morales à l'égard du traitement des données qui les concernent ne sont pas affectées par la présente directive;

(25) considérant que les principes de la protection doivent trouver leur expression, d'une part, dans les obligations mises à la charge des personnes, autorités publiques, entreprises, agences ou autres organismes qui traitent des données, ces obligations concernant en particulier la qualité des données, la sécurité technique, la notification à l'autorité de contrôle, les circonstances dans lesquelles le traitement peut être effectué, et, d'autre part, dans les droits donnés aux personnes dont les données font l'objet d'un traitement d'être informées sur celui-ci, de pouvoir accéder aux données, de pouvoir demander leur rectification, voire de s'opposer au traitement dans certaines circonstances;

(26) considérant que les principes de la protection doivent s'appliquer à toute information concernant une personne identifiée ou identifiable; que, pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en oeuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne; que les principes de la protection ne s'appliquent pas aux données rendues anonymes d'une manière telle que la personne concernée n'est plus identifiable; que les codes de conduite au sens de l'article 27 peuvent être un instrument utile pour fournir des indications sur les moyens par lesquels les données peuvent être rendues anonymes et conservées sous une forme ne permettant plus l'identification de la personne concernée;

(27) considérant que la protection des personnes doit s'appliquer aussi bien au traitement de données automatisé qu'au traitement manuel; que le champ de cette protection ne doit pas en effet dépendre des techniques utilisées, sauf à créer de graves risques de détournement; que, toutefois, s'agissant du traitement manuel, la présente directive ne couvre que les fichiers et ne s'applique pas aux dossiers non

structurés; que, en particulier, le contenu d'un fichier doit être structuré selon des critères déterminés relatifs aux personnes permettant un accès facile aux données à caractère personnel; que, conformément à la définition figurant à l'article 2 point c), les différents critères permettant de déterminer les éléments d'un ensemble structuré de données à caractère personnel et les différents critères régissant l'accès à cet ensemble de données peuvent être définis par chaque Etat membre; que les dossiers ou ensembles de dossiers, de même que leurs couvertures, qui ne sont pas structurés selon des critères déterminés n'entrent en aucun cas dans le champ d'application de la présente directive;

(28) considérant que tout traitement de données à caractère personnel doit être effectué licitement et loyalement à l'égard des personnes concernées; qu'il doit, en particulier, porter sur des données adéquates, pertinentes et non excessives au regard des finalités poursuivies; que ces finalités doivent être explicites et légitimes et doivent être déterminées lors de la collecte des données; que les finalités des traitements ultérieurs à la collecte ne peuvent pas être incompatibles avec les finalités telles que spécifiées à l'origine;

(29) considérant que le traitement ultérieur de données à caractère personnel à des fins historiques, statistiques ou scientifiques n'est pas considéré en général comme incompatible avec les finalités pour lesquelles les données ont été auparavant collectées, dans la mesure où les Etats membres prévoient des garanties appropriées; que ces garanties doivent notamment empêcher l'utilisation des données à l'appui de mesures ou de décisions prises à l'encontre d'une personne;

(30) considérant que, pour être licite, un traitement de données à caractère personnel doit en outre être fondé sur le consentement de la personne concernée ou être nécessaire à la conclusion ou à l'exécution d'un contrat liant la personne concernée, ou au respect d'une obligation légale, ou à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, ou encore à la réalisation d'un intérêt légitime d'une personne à condition que ne prévalent pas l'intérêt ou les droits et libertés de la personne concernée; que, en particulier, en vue d'assurer l'équilibre des intérêts en cause, tout en garantissant une concurrence effective, les Etats membres peuvent préciser les conditions dans lesquelles des données à caractère personnel peuvent être utilisées et communiquées à des tiers dans le cadre d'activités légitimes de gestion courante des entreprises et autres organismes; que, de même, ils peuvent préciser les conditions dans lesquelles la communication à des tiers de données à caractère personnel peut être effectuée à des fins de prospection commerciale, ou de prospection faite par une association à but caritatif ou par d'autres associations ou fondations, par exemple à caractère politique, dans le respect de dispositions visant à permettre aux personnes concernées de s'opposer sans devoir indiquer leurs motifs et sans frais au traitement des données les concernant;

(31) considérant qu'un traitement de données à caractère personnel doit être également considéré comme licite lorsqu'il est effectué en vue de protéger un intérêt essentiel à la vie de la personne concernée;

(32) considérant qu'il appartient aux législations nationales de déterminer si le responsable du traitement investi d'une mission d'intérêt public ou d'une mission relevant de l'exercice de l'autorité publique doit être une administration publique ou une autre personne soumise au droit public ou au droit privé, telle qu'une association professionnelle;

(33) considérant que les données qui sont susceptibles par leur nature de porter atteinte aux libertés fondamentales ou à la vie privée ne devraient pas faire l'objet d'un traitement, sauf consentement explicite de la personne concernée; que, cependant, des dérogations à cette interdiction doivent être expressément prévues pour répondre à des besoins spécifiques, en particulier lorsque le traitement de ces données est mis en oeuvre à certaines fins relatives à la santé par des personnes soumises à une obligation de secret professionnel ou pour la réalisation d'activités légitimes par certaines associations ou fondations dont l'objet est de permettre l'exercice de libertés fondamentales;

(34) considérant que les Etats membres doivent également être autorisés à déroger à l'interdiction de traiter des catégories de données sensibles lorsqu'un motif d'intérêt public important le justifie dans des domaines tels que la santé publique et la protection sociale - particulièrement afin d'assurer la qualité et la rentabilité en ce qui concerne les procédures utilisées pour régler les demandes de prestations et de services dans le régime d'assurance maladie - et tels que la recherche scientifique et les statistiques publiques; qu'il leur incombe, toutefois, de prévoir les garanties appropriées et spécifiques aux fins de protéger les droits fondamentaux et la vie privée des personnes;

(35) considérant, en outre, que le traitement de données à caractère personnel par des autorités publiques pour la réalisation de fins prévues par le droit constitutionnel ou le droit international public, au profit d'associations à caractère religieux officiellement reconnues, est mis en oeuvre pour un motif d'intérêt public important;

(36) considérant que, si, dans le cadre d'activités liées à des élections, le fonctionnement du système démocratique suppose, dans certains Etats membres, que les partis politiques collectent des données

relatives aux opinions politiques des personnes, le traitement de telles données peut être autorisé en raison de l'intérêt public important, à condition que des garanties appropriées soient prévues;

(37) considérant que le traitement de données à caractère personnel à des fins de journalisme ou d'expression artistique ou littéraire, notamment dans le domaine audiovisuel, doit bénéficier de dérogations ou de limitations de certaines dispositions de la présente directive dans la mesure où elles sont nécessaires à la conciliation des droits fondamentaux de la personne avec la liberté d'expression, et notamment la liberté de recevoir ou de communiquer des informations, telle que garantie notamment à l'article 10 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales; qu'il incombe donc aux Etats membres, aux fins de la pondération entre les droits fondamentaux, de prévoir les dérogations et limitations nécessaires en ce qui concerne les mesures générales relatives à la légalité du traitement des données, les mesures relatives au transfert des données vers des pays tiers ainsi que les compétences des autorités de contrôle, sans qu'il y ait lieu toutefois de prévoir des dérogations aux mesures visant à garantir la sécurité du traitement; qu'il conviendrait également de conférer au moins à l'autorité de contrôle compétente en la matière certaines compétences a posteriori, consistant par exemple à publier périodiquement un rapport ou à saisir les autorités judiciaires;

(38) considérant que le traitement loyal des données suppose que les personnes concernées puissent connaître l'existence des traitements et bénéficier, lorsque des données sont collectées auprès d'elles, d'une information effective et complète au regard des circonstances de cette collecte;

(39) considérant que certains traitements portent sur des données que le responsable n'a pas collectées directement auprès de la personne concernée; que, par ailleurs, des données peuvent être légitimement communiquées à un tiers, alors même que cette communication n'avait pas été prévue lors de la collecte des données auprès de la personne concernée; que, dans toutes ces hypothèses, l'information de la personne concernée doit se faire au moment de l'enregistrement des données ou, au plus tard, lorsque les données sont communiquées pour la première fois à un tiers;

(40) considérant que, cependant, il n'est pas nécessaire d'imposer cette obligation si la personne concernée est déjà informée; que, en outre, cette obligation n'est pas prévue si cet enregistrement ou cette communication sont expressément prévus par la loi ou si l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés, ce qui peut être le cas pour des traitements à des fins historiques, statistiques ou scientifiques; que, à cet égard, peuvent être pris en considération le nombre de personnes concernées, l'ancienneté des données, ainsi que les mesures compensatrices qui peuvent être prises;

(41) considérant que toute personne doit pouvoir bénéficier du droit d'accès aux données la concernant qui font l'objet d'un traitement, afin de s'assurer notamment de leur exactitude et de la licéité de leur traitement; que, pour les mêmes raisons, toute personne doit en outre avoir le droit de connaître la logique qui sous-tend le traitement automatisé des données la concernant, au moins dans le cas des décisions automatisées visées à l'article 15 paragraphe 1; que ce droit ne doit pas porter atteinte au secret des affaires ni à la propriété intellectuelle, notamment au droit d'auteur protégeant le logiciel; que cela ne doit toutefois pas aboutir au refus de toute information de la personne concernée;

(42) considérant que les Etats membres peuvent, dans l'intérêt de la personne concernée ou en vue de protéger les droits et libertés d'autrui, limiter les droits d'accès et d'information; qu'ils peuvent, par exemple, préciser que l'accès aux données à caractère médical ne peut être obtenu que par l'intermédiaire d'un professionnel de la santé;

(43) considérant que des restrictions aux droits d'accès et d'information, ainsi qu'à certaines obligations mises à la charge du responsable du traitement de données, peuvent également être prévues par les Etats membres dans la mesure où elles sont nécessaires à la sauvegarde, par exemple, de la sûreté de l'Etat, de la défense, de la sécurité publique, d'un intérêt économique ou financier important d'un Etat membre ou de l'Union européenne, ainsi qu'à la recherche et à la poursuite d'infractions pénales ou de manquements à la déontologie des professions réglementées; qu'il convient d'énumérer, au titre des exceptions et limitations, les missions de contrôle, d'inspection ou de réglementation nécessaires dans les trois derniers domaines précités concernant la sécurité publique, l'intérêt économique ou financier et la répression pénale; que cette énumération de missions concernant ces trois domaines n'affecte pas la légitimité d'exceptions et de restrictions pour des raisons de sûreté de l'Etat et de défense;

(44) considérant que les Etats membres peuvent être amenés, en vertu de dispositions du droit communautaire, à déroger aux dispositions de la présente directive concernant le droit d'accès, l'information des personnes et la qualité des données, afin de sauvegarder certaines finalités parmi celles visées ci-dessus;

(45) considérant que, dans le cas où des données pourraient faire l'objet d'un traitement licite sur le fondement d'un intérêt public, de l'exercice de l'autorité publique ou de l'intérêt légitime d'une personne,

toute personne concernée devrait, toutefois, avoir le droit de s'opposer, pour des raisons prépondérantes et légitimes tenant à sa situation particulière, à ce que les données la concernant fassent l'objet d'un traitement; que les Etats membres ont, néanmoins, la possibilité de prévoir des dispositions nationales contraires;

(46) considérant que la protection des droits et libertés des personnes concernées à l'égard du traitement de données à caractère personnel exige que des mesures techniques et d'organisation appropriées soient prises tant au moment de la conception qu'à celui de la mise en oeuvre du traitement, en vue d'assurer en particulier la sécurité et d'empêcher ainsi tout traitement non autorisé; qu'il incombe aux Etats membres de veiller au respect de ces mesures par les responsables du traitement; que ces mesures doivent assurer un niveau de sécurité approprié tenant compte de l'état de l'art et du coût de leur mise en oeuvre au regard des risques présentés par les traitements et de la nature des données à protéger;

(47) considérant que, lorsqu'un message contenant des données à caractère personnel est transmis via un service de télécommunications ou de courrier électronique dont le seul objet est de transmettre des messages de ce type, c'est la personne dont émane le message, et non celle qui offre le service de transmission, qui sera normalement considérée comme responsable du traitement de données à caractère personnel contenues dans le message; que, toutefois, les personnes qui offrent ces services seront normalement considérées comme responsables du traitement des données à caractère personnel supplémentaires nécessaires au fonctionnement du service;

(48) considérant que la notification à l'autorité de contrôle a pour objet d'organiser la publicité des finalités du traitement, ainsi que de ses principales caractéristiques, en vue de son contrôle au regard des dispositions nationales prises en application de la présente directive;

(49) considérant que, afin d'éviter des formalités administratives inadéquates, des exonérations ou des simplifications de la notification peuvent être prévues par les Etats membres pour les traitements de données qui ne sont pas susceptibles de porter atteinte aux droits et libertés des personnes concernées, à condition qu'ils soient conformes à un acte pris par l'Etat membre qui en précise les limites; que des exonérations ou simplifications peuvent pareillement être prévues par les Etats membres dès lors qu'une personne désignée par le responsable du traitement de données s'assure que les traitements effectués ne sont pas susceptibles de porter atteinte aux droits et libertés des personnes concernées; que la personne ainsi détachée à la protection des données, employée ou non du responsable du traitement de données, doit être en mesure d'exercer ses fonctions en toute indépendance;

(50) considérant que des exonérations ou simplifications peuvent être prévues pour le traitement de données dont le seul but est de tenir un registre destiné, dans le respect du droit national, à l'information du public et qui est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime;

(51) considérant que, néanmoins, le bénéfice de la simplification ou de l'exonération de l'obligation de notification ne dispense le responsable du traitement de données d'aucune des autres obligations découlant de la présente directive;

(52) considérant que, dans ce contexte, le contrôle a posteriori par les autorités compétentes doit être en général considéré comme une mesure suffisante;

(53) considérant que, cependant, certains traitements sont susceptibles de présenter des risques particuliers au regard des droits et des libertés des personnes concernées, du fait de leur nature, de leur portée ou de leurs finalités telles que celle d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat, ou du fait de l'usage particulier d'une technologie nouvelle; qu'il appartient aux Etats membres, s'ils le souhaitent, de préciser dans leur législation de tels risques;

(54) considérant que, au regard de tous les traitements mis en oeuvre dans la société, le nombre de ceux présentant de tels risques particuliers devrait être très restreint; que les Etats membres doivent prévoir, pour ces traitements, un examen préalable à leur mise en oeuvre, effectué par l'autorité de contrôle ou par le détaché à la protection des données en coopération avec celle-ci; que, à la suite de cet examen préalable, l'autorité de contrôle peut, selon le droit national dont elle relève, émettre un avis ou autoriser le traitement des données; qu'un tel examen peut également être effectué au cours de l'élaboration soit d'une mesure législative du Parlement national, soit d'une mesure fondée sur une telle mesure législative, qui définisse la nature du traitement et précise les garanties appropriées;

(55) considérant que, en cas de non-respect des droits des personnes concernées par le responsable du traitement de données, un recours juridictionnel doit être prévu par les législations nationales; que les dommages que peuvent subir les personnes du fait d'un traitement illicite doivent être réparés par le responsable du traitement de données, lequel peut être exonéré de sa responsabilité s'il prouve que le fait dommageable ne lui est pas imputable, notamment lorsqu'il établit l'existence d'une faute de la personne concernée ou d'un cas de force majeure; que des sanctions doivent être appliquées à toute personne, tant de droit

privé que de droit public, qui ne respecte pas les dispositions nationales prises en application de la présente directive;

(56) considérant que des flux transfrontaliers de données à caractère personnel sont nécessaires au développement du commerce international; que la protection des personnes garantie dans la Communauté par la présente directive ne s'oppose pas aux transferts de données à caractère personnel vers des pays tiers assurant un niveau de protection adéquat; que le caractère adéquat du niveau de protection offert par un pays tiers doit s'apprécier au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts;

(57) considérant, en revanche, que, lorsqu'un pays tiers n'offre pas un niveau de protection adéquat, le transfert de données à caractère personnel vers ce pays doit être interdit;

(58) considérant que des exceptions à cette interdiction doivent pouvoir être prévues dans certaines circonstances lorsque la personne concernée a donné son consentement, lorsque le transfert est nécessaire dans le contexte d'un contrat ou d'une action en justice, lorsque la sauvegarde d'un intérêt public important l'exige, par exemple en cas d'échanges internationaux de données entre les administrations fiscales ou douanières ou entre les services compétents en matière de sécurité sociale, ou lorsque le transfert est effectué à partir d'un registre établi par la loi et destiné à être consulté par le public ou par des personnes ayant un intérêt légitime; que, dans ce cas, un tel transfert ne devrait pas porter sur la totalité des données ni sur des catégories de données contenues dans ce registre; que, lorsqu'un registre est destiné à être consulté par des personnes qui ont un intérêt légitime, le transfert ne devrait pouvoir être effectué qu'à la demande de ces personnes ou lorsqu'elles en sont les destinataires;

(59) considérant que des mesures particulières peuvent être prises pour pallier l'insuffisance du niveau de protection dans un pays tiers lorsque le responsable du traitement présente des garanties appropriées; que, en outre, des procédures de négociation entre la Communauté et les pays tiers en cause doivent être prévues;

(60) considérant que, en tout état de cause, les transferts vers les pays tiers ne peuvent être effectués que dans le plein respect des dispositions prises par les Etats membres en application de la présente directive, et notamment de son article 8;

(61) considérant que les Etats membres et la Commission, dans leurs domaines de compétence respectifs, doivent encourager les milieux professionnels concernés à élaborer des codes de conduite en vue de favoriser, compte tenu des spécificités du traitement de données effectué dans certains secteurs, la mise en oeuvre de la présente directive dans le respect des dispositions nationales prises pour son application;

(62) considérant que l'institution, dans les Etats membres, d'autorités de contrôle exerçant en toute indépendance leurs fonctions est un élément essentiel de la protection des personnes à l'égard du traitement des données à caractère personnel;

(63) considérant que ces autorités doivent être dotées des moyens nécessaires à l'exécution de leurs tâches, qu'il s'agisse des pouvoirs d'investigation et d'intervention, en particulier lorsque les autorités sont saisies de réclamations, ou du pouvoir d'ester en justice; qu'elles doivent contribuer à la transparence du traitement de données effectué dans l'Etat membre dont elles relèvent;

(64) considérant que les autorités des différents Etats membres seront appelées à se prêter mutuellement assistance dans la réalisation de leurs tâches afin d'assurer le plein respect des règles de protection dans l'Union européenne;

(65) considérant que, au niveau communautaire, un groupe de travail sur la protection des personnes à l'égard du traitement des données à caractère personnel doit être instauré et qu'il doit exercer ses fonctions en toute indépendance; que, compte tenu de cette spécificité, il doit conseiller la Commission et contribuer notamment à l'application homogène des règles nationales adoptées en application de la présente directive;

(66) considérant que, pour ce qui est du transfert de données vers les pays tiers, l'application de la présente directive nécessite l'attribution de compétences d'exécution à la Commission et l'établissement d'une procédure selon les modalités fixées dans la décision 87/373/CEE du Conseil¹;

(67) considérant qu'un accord sur un *modus vivendi* concernant les mesures d'exécution des actes arrêtés selon la procédure visée à l'article 189 B du traité est intervenu, le 20 décembre 1994, entre le Parlement européen, le Conseil et la Commission;

(68) considérant que les principes énoncés dans la présente directive et régissant la protection des droits et des libertés des personnes, notamment du droit à la vie privée, à l'égard du traitement des données à

¹ JO n° L 197 du 18. 7. 1987, p. 33.

caractère personnel pourront être complétés ou précisés, notamment pour certains secteurs, par des règles spécifiques conformes à ces principes;

(69) considérant qu'il convient de laisser aux Etats membres un délai ne pouvant pas excéder trois ans à compter de l'entrée en vigueur des mesures nationales de transposition de la présente directive, pour leur permettre d'appliquer progressivement à tout traitement de données déjà mis en oeuvre les nouvelles dispositions nationales susvisées; que, afin de permettre un bon rapport coût-efficacité lors de la mise en oeuvre de ces dispositions, les Etats membres sont autorisés à prévoir une période supplémentaire, expirant douze ans après la date d'adoption de la présente directive, pour la mise en conformité des fichiers manuels existants avec certaines dispositions de la directive; que, lorsque des données contenues dans de tels fichiers font l'objet d'un traitement manuel effectif pendant cette période transitoire supplémentaire, la mise en conformité avec ces dispositions doit être effectuée au moment de la réalisation de ce traitement;

(70) considérant qu'il n'y a pas lieu que la personne concernée donne à nouveau son consentement pour permettre au responsable de continuer à effectuer, après l'entrée en vigueur des dispositions nationales prises en application de la présente directive, un traitement de données sensibles nécessaire à l'exécution d'un contrat conclu sur la base d'un consentement libre et informé avant l'entrée en vigueur des dispositions précitées;

(71) considérant que la présente directive ne s'oppose pas à ce qu'un Etat membre réglemente les activités de prospection commerciale visant les consommateurs qui résident sur son territoire, dans la mesure où cette réglementation ne concerne pas la protection des personnes à l'égard du traitement de données à caractère personnel;

(72) considérant que la présente directive permet de prendre en compte, dans la mise en oeuvre des règles qu'elle pose, le principe du droit d'accès du public aux documents administratifs,

Ont arrêté la présente directive:

Chapitre I^{er}. - Dispositions générales

Art. 1^{er}. Objet de la directive

1. Les Etats membres assurent, conformément à la présente directive, la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel.

2. Les Etats membres ne peuvent restreindre ni interdire la libre circulation des données à caractère personnel entre Etats membres pour des raisons relatives à la protection assurée en vertu du paragraphe 1^{er}.

Art. 2. Définitions

Aux fins de la présente directive, on entend par:

a) «données à caractère personnel»: toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale;

b) «traitement de données à caractère personnel» (traitement): toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction;

c) «fichier de données à caractère personnel» (fichier): tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique;

d) «responsable du traitement»: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel; lorsque les finalités et les moyens du traitement sont déterminés par des dispositions législatives ou réglementaires nationales ou communautaires, le responsable du traitement ou les critères spécifiques pour le désigner peuvent être fixés par le droit national ou communautaire;

e) «sous-traitement»: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement;

f) «tiers»: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilitées à traiter les données;

g) «destinataire»: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données, qu'il s'agisse ou non d'un tiers; les autorités qui sont susceptibles de recevoir communication de données dans le cadre d'une mission d'enquête particulière ne sont toutefois pas considérées comme des destinataires;

h) «consentement de la personne concernée»: toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Art. 3. Champ d'application

1. La présente directive s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.

2. La présente directive ne s'applique pas au traitement de données à caractère personnel:

- mis en oeuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telles que celles prévues aux titres V et VI du traité sur l'Union européenne, et, en tout état de cause, aux traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'Etat (y compris le bien-être économique de l'Etat lorsque ces traitements sont liés à des questions de sûreté de l'Etat) et les activités de l'Etat relatives à des domaines du droit pénal,
- effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques.

Art. 4. Droit national applicable

1. Chaque Etat membre applique les dispositions nationales qu'il arrête en vertu de la présente directive aux traitements de données à caractère personnel lorsque:

- a) le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'Etat membre; si un même responsable du traitement est établi sur le territoire de plusieurs Etats membres, il doit prendre les mesures nécessaires pour assurer le respect, par chacun de ses établissements, des obligations prévues par le droit national applicable;
- b) le responsable du traitement n'est pas établi sur le territoire de l'Etat membre mais en un lieu où sa loi nationale s'applique en vertu du droit international public;
- c) le responsable du traitement n'est pas établi sur le territoire de la Communauté et recourt, à des fins de traitement de données à caractère personnel, à des moyens, automatisés ou non, situés sur le territoire dudit Etat membre, sauf si ces moyens ne sont utilisés qu'à des fins de transit sur le territoire de la Communauté.

2. Dans le cas visé au paragraphe 1 point c), le responsable du traitement doit désigner un représentant établi sur le territoire dudit Etat membre, sans préjudice d'actions qui pourraient être introduites contre le responsable du traitement lui-même.

Chapitre II. - Conditions générales de licéité des traitements de données à caractère personnel

Art. 5.

Les Etats membres précisent, dans les limites des dispositions du présent chapitre, les conditions dans lesquelles les traitements de données à caractère personnel sont licites.

Section 1^{er}. Principes relatifs à la qualité des données

Art. 6

1. Les Etats membres prévoient que les données à caractère personnel doivent être:

- a) traitées loyalement et licitement;

- b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. Un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible pour autant que les Etats membres prévoient des garanties appropriées;
 - c) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement;
 - d) exactes et, si nécessaire, mises à jour; toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées;
 - e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement. Les Etats membres prévoient des garanties appropriées pour les données à caractère personnel qui sont conservées au-delà de la période précitée, à des fins historiques, statistiques ou scientifiques.
2. Il incombe au responsable du traitement d'assurer le respect du paragraphe 1^{er}.

Section II. Principes relatifs à la légitimation des traitements de données

Art. 7.

Les Etats membres prévoient que le traitement de données à caractère personnel ne peut être effectué que si:

- a) la personne concernée a indubitablement donné son consentement ou
- b) il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ou
- c) il est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ou
- d) il est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée ou
- e) il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées ou
- f) il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1^{er} paragraphe 1^{er}.

Section III. Catégories particulières de traitements

Art. 8. Traitements portant sur des catégories particulières de données

1. Les Etats membres interdisent le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle.

2. Le paragraphe 1^{er} ne s'applique pas lorsque:

- a) la personne concernée a donné son consentement explicite à un tel traitement, sauf dans le cas où la législation de l'Etat membre prévoit que l'interdiction visée au paragraphe 1^{er} ne peut être levée par le consentement de la personne concernée ou
- b) le traitement est nécessaire aux fins de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail, dans la mesure où il est autorisé par une législation nationale prévoyant des garanties adéquates ou
- c) le traitement est nécessaire à la défense des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ou
- d) le traitement est effectué dans le cadre de leurs activités légitimes et avec des garanties appropriées par une fondation, une association ou tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale, à condition que le traitement se rapporte aux seuls membres de cet organisme ou aux personnes entretenant avec lui des contacts réguliers liés à sa finalité et que

les données ne soient pas communiquées à des tiers sans le consentement des personnes concernées ou

- e) le traitement porte sur des données manifestement rendues publiques par la personne concernée ou est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice.

3. Le paragraphe 1^{er} ne s'applique pas lorsque le traitement des données est nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion de services de santé et que le traitement de ces données est effectué par un praticien de la santé soumis par le droit national ou par des réglementations arrêtées par les autorités nationales compétentes au secret professionnel, ou par une autre personne également soumise à une obligation de secret équivalente.

4. Sous réserve de garanties appropriées, les Etats membres peuvent prévoir, pour un motif d'intérêt public important, des dérogations autres que celles prévues au paragraphe 2, soit par leur législation nationale, soit sur décision de l'autorité de contrôle.

5. Le traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peut être effectué que sous le contrôle de l'autorité publique ou si des garanties appropriées et spécifiques sont prévues par le droit national, sous réserve des dérogations qui peuvent être accordées par l'Etat membre sur la base de dispositions nationales prévoyant des garanties appropriées et spécifiques. Toutefois, un recueil exhaustif des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique.

Les Etats membres peuvent prévoir que les données relatives aux sanctions administratives ou aux jugements civils sont également traitées sous le contrôle de l'autorité publique.

6. Les dérogations au paragraphe 1^{er} prévues aux paragraphes 4 et 5 sont notifiées à la Commission.

7. Les Etats membres déterminent les conditions dans lesquelles un numéro national d'identification ou tout autre identifiant de portée générale peut faire l'objet d'un traitement.

Art. 9. Traitements de données à caractère personnel et liberté d'expression

Les Etats membres prévoient, pour les traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression artistique ou littéraire, des exemptions et dérogations au présent chapitre, au chapitre IV et au chapitre VI dans la seule mesure où elles s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression.

Section IV. Information de la personne concernée

Art. 10. Informations en cas de collecte de données auprès de la personne concernée

Les Etats membres prévoient que le responsable du traitement ou son représentant doit fournir à la personne auprès de laquelle il collecte des données la concernant au moins les informations énumérées ci-dessous, sauf si la personne en est déjà informée:

- a) l'identité du responsable du traitement et, le cas échéant, de son représentant;
- b) les finalités du traitement auquel les données sont destinées;
- c) toute information supplémentaire telle que:
 - les destinataires ou les catégories de destinataires des données,
 - le fait de savoir si la réponse aux questions est obligatoire ou facultative ainsi que les conséquences éventuelles d'un défaut de réponse,
 - l'existence d'un droit d'accès aux données la concernant et de rectification de ces données,

dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données.

Art. 11. Informations lorsque les données n'ont pas été collectées auprès de la personne concernée

1. Lorsque les données n'ont pas été collectées auprès de la personne concernée, les Etats membres prévoient que le responsable du traitement ou son représentant doit, dès l'enregistrement des données ou, si une communication de données à un tiers est envisagée, au plus tard lors de la première communication de données, fournir à la personne concernée au moins les informations énumérées ci-dessous, sauf si la personne en est déjà informée:

- a) l'identité du responsable du traitement et, le cas échéant, de son représentant;

b) les finalités du traitement;

c) toute information supplémentaire telle que:

- les catégories de données concernées,
- les destinataires ou les catégories de destinataires des données,
- l'existence d'un droit d'accès aux données la concernant et de rectification de ces données,

dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données.

2. Le paragraphe 1^{er} ne s'applique pas lorsque, en particulier pour un traitement à finalité statistique ou de recherche historique ou scientifique, l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés ou si la législation prévoit expressément l'enregistrement ou la communication des données. Dans ces cas, les Etats membres prévoient des garanties appropriées.

Section V. Droit d'accès de la personne concernée aux données

Art. 12. Droit d'accès

Les Etats membres garantissent à toute personne concernée le droit d'obtenir du responsable du traitement:

a) sans contrainte, à des intervalles raisonnables et sans délais ou frais excessifs:

- la confirmation que des données la concernant sont ou ne sont pas traitées, ainsi que des informations portant au moins sur les finalités du traitement, les catégories de données sur lesquelles il porte et les destinataires ou les catégories de destinataires auxquels les données sont communiquées,
- la communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine des données,
- la connaissance de la logique qui sous-tend tout traitement automatisé des données la concernant, au moins dans le cas des décisions automatisées visées à l'article 15 paragraphe 1^{er};

b) selon le cas, la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la présente directive, notamment en raison du caractère incomplet ou inexact des données;

c) la notification aux tiers auxquels les données ont été communiquées de toute rectification, tout effacement ou tout verrouillage effectué conformément au point b), si cela ne s'avère pas impossible ou ne suppose pas un effort disproportionné.

Section VI. Exceptions et limitations

Art. 13. Exceptions et limitations

1. Les Etats membres peuvent prendre des mesures législatives visant à limiter la portée des obligations et des droits prévus à l'article 6 paragraphe 1, à l'article 10, à l'article 11 paragraphe 1^{er} et aux articles 12 et 21, lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder:

- a) la sûreté de l'Etat;
- b) la défense;
- c) la sécurité publique;
- d) la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de manquements à la déontologie dans le cas des professions réglementées;
- e) un intérêt économique ou financier important d'un Etat membre ou de l'Union européenne, y compris dans les domaines monétaire, budgétaire et fiscal;
- f) une mission de contrôle, d'inspection ou de réglementation relevant, même à titre occasionnel, de l'exercice de l'autorité publique, dans les cas visés aux points c), d) et e);
- g) la protection de la personne concernée ou des droits et libertés d'autrui.

2. Sous réserve de garanties légales appropriées, excluant notamment que les données puissent être utilisées aux fins de mesures ou de décisions se rapportant à des personnes précises, les Etats membres peuvent, dans le cas où il n'existe manifestement aucun risque d'atteinte à la vie privée de la personne concernée, limiter par une mesure législative les droits prévus à l'article 12 lorsque les données sont traitées exclusivement aux fins de la recherche scientifique ou sont stockées sous la forme de données à caractère personnel pendant une durée n'excédant pas celle nécessaire à la seule finalité d'établissement de statistiques.

*Section VII. Droit d'opposition de la personne concernée***Art. 14. Droit d'opposition de la personne concernée**

Les Etats membres reconnaissent à la personne concernée le droit:

- a) au moins dans les cas visés à l'article 7 points e) et f), de s'opposer à tout moment, pour des raisons prépondérantes et légitimes tenant à sa situation particulière, à ce que des données la concernant fassent l'objet d'un traitement, sauf en cas de disposition contraire du droit national. En cas d'opposition justifiée, le traitement mis en oeuvre par le responsable du traitement ne peut plus porter sur ces données;
- b) de s'opposer, sur demande et gratuitement, au traitement des données à caractère personnel la concernant envisagé par le responsable du traitement à des fins de prospection ou d'être informée avant que des données à caractère personnel ne soient pour la première fois communiquées à des tiers ou utilisées pour le compte de tiers à des fins de prospection et de se voir expressément offrir le droit de s'opposer, gratuitement, à ladite communication ou utilisation.

Les Etats membres prennent les mesures nécessaires pour garantir que les personnes concernées ont connaissance de l'existence du droit visé au point b) premier alinéa.

Art. 15. Décisions individuelles automatisées

1. Les Etats membres reconnaissent à toute personne le droit de ne pas être soumise à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité, tels que son rendement professionnel, son crédit, sa fiabilité, son comportement, etc.

2. Les Etats membres prévoient, sous réserve des autres dispositions de la présente directive, qu'une personne peut être soumise à une décision telle que celle visée au paragraphe 1^{er} si une telle décision:

- a) est prise dans le cadre de la conclusion ou de l'exécution d'un contrat, à condition que la demande de conclusion ou d'exécution du contrat, introduite par la personne concernée, ait été satisfaite ou que des mesures appropriées, telles que la possibilité de faire valoir son point de vue, garantissent la sauvegarde de son intérêt légitime ou
- b) est autorisée par une loi qui précise les mesures garantissant la sauvegarde de l'intérêt légitime de la personne concernée.

*Section VIII. Confidentialité et sécurité des traitements***Art. 16. Confidentialité des traitements**

Toute personne agissant sous l'autorité du responsable du traitement ou celle du sous-traitant, ainsi que le sous-traitant lui-même, qui accède à des données à caractère personnel ne peut les traiter que sur instruction du responsable du traitement, sauf en vertu d'obligations légales.

Art. 17. Sécurité des traitements

1. Les Etats membres prévoient que le responsable du traitement doit mettre en oeuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite.

Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en oeuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger.

2. Les Etats membres prévoient que le responsable du traitement, lorsque le traitement est effectué pour son compte, doit choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer et qu'il doit veiller au respect de ces mesures.

3. La réalisation de traitements en sous-traitance doit être régie par un contrat ou un acte juridique qui lie le sous-traitant au responsable du traitement et qui prévoit notamment que:

- le sous-traitant n'agit que sur la seule instruction du responsable du traitement,
- les obligations visées au paragraphe 1^{er}, telles que définies par la législation de l'Etat membre dans lequel le sous-traitant est établi, incombent également à celui-ci.

4. Aux fins de la conservation des preuves, les éléments du contrat ou de l'acte juridique relatifs à la protection des données et les exigences portant sur les mesures visées au paragraphe 1 sont consignés par écrit ou sous une autre forme équivalente.

Section IX. Notification

Art. 18. Obligation de notification à l'autorité de contrôle

1. Les Etats membres prévoient que le responsable du traitement, ou le cas échéant son représentant, doit adresser une notification à l'autorité de contrôle visée à l'article 28 préalablement à la mise en oeuvre d'un traitement entièrement ou partiellement automatisé ou d'un ensemble de tels traitements ayant une même finalité ou des finalités liées.

2. Les Etats membres ne peuvent prévoir de simplification de la notification ou de dérogation à cette obligation que dans les cas et aux conditions suivants:

- lorsque, pour les catégories de traitement qui, compte tenu des données à traiter, ne sont pas susceptibles de porter atteinte aux droits et libertés des personnes concernées, ils précisent les finalités des traitements, les données ou catégories de données traitées, la ou les catégories de personnes concernées, les destinataires ou catégories de destinataires auxquels les données sont communiquées et la durée de conservation des données et/ou
- lorsque le responsable du traitement désigne, conformément au droit national auquel il est soumis, un détaché à la protection des données à caractère personnel chargé notamment:
 - d'assurer, d'une manière indépendante, l'application interne des dispositions nationales prises en application de la présente directive,
 - de tenir un registre des traitements effectués par le responsable du traitement, contenant les informations visées à l'article 21 paragraphe 2, et garantissant de la sorte que les traitements ne sont pas susceptibles de porter atteinte faux droits et libertés des personnes concernées.

3. Les Etats membres peuvent prévoir que le paragraphe 1^{er} ne s'applique pas aux traitements ayant pour seul objet la tenue d'un registre qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime.

4. Les Etats membres peuvent prévoir une dérogation à l'obligation de notification ou une simplification de la notification pour les traitements visés à l'article 8 paragraphe 2 point d).

5. Les Etats membres peuvent prévoir que les traitements non automatisés de données à caractère personnel, ou certains d'entre eux, font l'objet d'une notification, éventuellement simplifiée.

Art. 19. Contenu de la notification

1. Les Etats membres précisent les informations qui doivent figurer dans la notification. Elles comprennent au minimum:

- a) le nom et l'adresse du responsable du traitement et, le cas échéant, de son représentant;
- b) la ou les finalités du traitement;
- c) une description de la ou des catégories de personnes concernées et des données ou des catégories de données s'y rapportant;
- d) les destinataires ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées;
- e) les transferts de données envisagés à destination de pays tiers;
- f) une description générale permettant d'apprécier de façon préliminaire le caractère approprié des mesures prises pour assurer la sécurité du traitement en application de l'article 17.

2. Les Etats membres précisent les modalités de notification à l'autorité de contrôle des changements affectant les informations visées au paragraphe 1^{er}.

Art. 20. Contrôles préalables

1. Les Etats membres précisent les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées et veillent à ce que ces traitements soient examinés avant leur mise en oeuvre.

2. De tels examens préalables sont effectués par l'autorité de contrôle après réception de la notification du responsable du traitement ou par le détaché à la protection des données, qui, en cas de doute, doit consulter l'autorité de contrôle.

3. Les Etats membres peuvent aussi procéder à un tel examen dans le cadre de l'élaboration soit d'une mesure du Parlement national, soit d'une mesure fondée sur une telle mesure législative, qui définisse la nature du traitement et fixe des garanties appropriées.

Art. 21. Publicité des traitements

1. Les Etats membres prennent des mesures pour assurer la publicité des traitements.

2. Les Etats membres prévoient que l'autorité de contrôle tient un registre des traitements notifiés en vertu de l'article 18.

Le registre contient au minimum les informations énumérées à l'article 19 paragraphe 1 points a) à e).

Le registre peut être consulté par toute personne.

3. En ce qui concerne les traitements non soumis à notification, les Etats membres prévoient que le responsable du traitement ou une autre instance qu'ils désignent communique sous une forme appropriée à toute personne qui en fait la demande au moins les informations visées à l'article 19 paragraphe 1 points a) à e).

Les Etats membres peuvent prévoir que la présente disposition ne s'applique pas aux traitements ayant pour seul objet la tenue d'un registre qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime.

Chapitre III. - Recours juridictionnels, responsabilité et sanctions

Art. 22. Recours

Sans préjudice du recours administratif qui peut être organisé, notamment devant l'autorité de contrôle visée à l'article 28, antérieurement à la saisine de l'autorité judiciaire, les Etats membres prévoient que toute personne dispose d'un recours juridictionnel en cas de violation des droits qui lui sont garantis par les dispositions nationales applicables au traitement en question.

Art. 23. Responsabilité

1. Les Etats membres prévoient que toute personne ayant subi un dommage du fait d'un traitement illicite ou de toute action incompatible avec les dispositions nationales prises en application de la présente directive a le droit d'obtenir du responsable du traitement réparation du préjudice subi.

2. Le responsable du traitement peut être exonéré partiellement ou totalement de cette responsabilité s'il prouve que le fait qui a provoqué le dommage ne lui est pas imputable.

Art. 24. Sanctions

Les Etats membres prennent les mesures appropriées pour assurer la pleine application des dispositions de la présente directive et déterminent notamment les sanctions à appliquer en cas de violation des dispositions prises en application de la présente directive.

Chapitre IV. - Transfert de données à caractère personnel vers des pays tiers

Art. 25. Principes

1. Les Etats membres prévoient que le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement après leur transfert, ne peut avoir lieu que si, sous réserve du respect des dispositions nationales prises en application des autres dispositions de la présente directive, le pays tiers en question assure un niveau de protection adéquat.

2. Le caractère adéquat du niveau de protection offert par un pays tiers s'apprécie au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données; en particulier, sont prises en considération la nature des données, la finalité et la durée du ou des traitements envisagés, les pays d'origine et de destination finale, les règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées.

3. Les Etats membres et la Commission s'informent mutuellement des cas dans lesquels ils estiment qu'un pays tiers n'assure pas un niveau de protection adéquat au sens du paragraphe 2.

4. Lorsque la Commission constate, conformément à la procédure prévue à l'article 31 paragraphe 2, qu'un pays tiers n'assure pas un niveau de protection adéquat au sens du paragraphe 2 du présent article, les Etats membres prennent les mesures nécessaires en vue d'empêcher tout transfert de même nature vers le pays tiers en cause.

5. La Commission engage, au moment opportun, des négociations en vue de remédier à la situation résultant de la constatation faite en application du paragraphe 4.

6. La Commission peut constater, conformément à la procédure prévue à l'article 31 paragraphe 2, qu'un pays tiers assure un niveau de protection adéquat au sens du paragraphe 2 du présent article, en raison de sa législation interne ou de ses engagements internationaux, souscrits notamment à l'issue des négociations visées au paragraphe 5, en vue de la protection de la vie privée et des libertés et droits fondamentaux des personnes.

Les Etats membres prennent les mesures nécessaires pour se conformer à la décision de la Commission.

Art. 26. Dérogations

1. Par dérogation à l'article 25 et sous réserve de dispositions contraires de leur droit national régissant des cas particuliers, les Etats membres prévoient qu'un transfert de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat au sens de l'article 25 paragraphe 2 peut être effectué, à condition que:

- a) la personne concernée ait indubitablement donné son consentement au transfert envisagé ou
- b) le transfert soit nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à l'exécution de mesures précontractuelles prises à la demande de la personne concernée ou
- c) le transfert soit nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers ou
- d) le transfert soit nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice ou
- e) le transfert soit nécessaire à la sauvegarde de l'intérêt vital de la personne concernée ou
- f) le transfert intervienne au départ d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime, dans la mesure où les conditions légales pour la consultation sont remplies dans le cas particulier.

2. Sans préjudice du paragraphe 1^{er}, un Etat membre peut autoriser un transfert, ou un ensemble de transferts, de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat au sens de l'article 25 paragraphe 2, lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants; ces garanties peuvent notamment résulter de clauses contractuelles appropriées.

3. L'Etat membre informe la Commission et les autres Etats membres des autorisations qu'il accorde en application du paragraphe 2.

En cas d'opposition exprimée par un autre Etat membre ou par la Commission et dûment justifiée au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, la Commission arrête les mesures appropriées, conformément à la procédure prévue à l'article 31 paragraphe 2.

Les Etats membres prennent les mesures nécessaires pour se conformer à la décision de la Commission.

4. Lorsque la Commission décide, conformément à la procédure prévue à l'article 31 paragraphe 2, que certaines clauses contractuelles types présentent les garanties suffisantes visées au paragraphe 2, les Etats membres prennent les mesures nécessaires pour se conformer à la décision de la Commission.

Chapitre V. - Codes de conduite

Art. 27.

1. Les Etats membres et la Commission encouragent l'élaboration de codes de conduite destinés à contribuer, en fonction de la spécificité des secteurs, à la bonne application des dispositions nationales prises par les Etats membres en application de la présente directive.

2. Les Etats membres prévoient que les associations professionnelles et les autres organisations représentant d'autres catégories de responsables du traitement qui ont élaboré des projets de codes nationaux ou qui ont l'intention de modifier ou de proroger des codes nationaux existants peuvent les soumettre à l'examen de l'autorité nationale.

Les Etats membres prévoient que cette autorité s'assure, entre autres, de la conformité des projets qui lui sont soumis avec les dispositions nationales prises en application de la présente directive. Si elle l'estime opportun, l'autorité recueille les observations des personnes concernées ou de leurs représentants.

3. Les projets de codes communautaires, ainsi que les modifications ou prorogations de codes communautaires existants, peuvent être soumis au groupe visé à l'article 29. Celui-ci se prononce, entre autres, sur la conformité des projets qui lui sont soumis avec les dispositions nationales prises en application de la présente directive. S'il l'estime opportun, il recueille les observations des personnes concernées ou de leurs représentants. La Commission peut assurer une publicité appropriée aux codes qui ont été approuvés par le groupe.

Chapitre VI. - Autorité de contrôle et groupe de protection des personnes à l'égard du traitement des données à caractère personnel

Art. 28. Autorité de contrôle

1. Chaque Etat membre prévoit qu'une ou plusieurs autorités publiques sont chargées de surveiller l'application, sur son territoire, des dispositions adoptées par les Etats membres en application de la présente directive.

Ces autorités exercent en toute indépendance les missions dont elles sont investies.

2. Chaque Etat membre prévoit que les autorités de contrôle sont consultées lors de l'élaboration des mesures réglementaires ou administratives relatives à la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel.

3. Chaque autorité de contrôle dispose notamment:

- de pouvoirs d'investigation, tels que le pouvoir d'accéder aux données faisant l'objet d'un traitement et de recueillir toutes les informations nécessaires à l'accomplissement de sa mission de contrôle,
- de pouvoirs effectifs d'intervention, tels que, par exemple, celui de rendre des avis préalablement à la mise en oeuvre des traitements, conformément à l'article 20, et d'assurer une publication appropriée de ces avis ou celui d'ordonner le verrouillage, l'effacement ou la destruction de données, ou d'interdire temporairement ou définitivement un traitement, ou celui d'adresser un avertissement ou une admonestation au responsable du traitement ou celui de saisir les parlements nationaux ou d'autres institutions politiques,
- du pouvoir d'ester en justice en cas de violation des dispositions nationales prises en application de la présente directive ou du pouvoir de porter ces violations à la connaissance de l'autorité judiciaire.

Les décisions de l'autorité de contrôle faisant grief peuvent faire l'objet d'un recours juridictionnel.

4. Chaque autorité de contrôle peut être saisie par toute personne, ou par une association la représentant, d'une demande relative à la protection de ses droits et libertés à l'égard du traitement de données à caractère personnel. La personne concernée est informée des suites données à sa demande.

Chaque autorité de contrôle peut, en particulier, être saisie par toute personne d'une demande de vérification de la licéité d'un traitement lorsque les dispositions nationales prises en vertu de l'article 13 de la présente directive sont d'application. La personne est à tout le moins informée de ce qu'une vérification a eu lieu.

5. Chaque autorité de contrôle établit à intervalles réguliers un rapport sur son activité. Ce rapport est publié.

6. Indépendamment du droit national applicable au traitement en cause, chaque autorité de contrôle a compétence pour exercer, sur le territoire de l'Etat membre dont elle relève, les pouvoirs dont elle est investie conformément au paragraphe 3. Chaque autorité peut être appelée à exercer ses pouvoirs sur demande d'une autorité d'un autre Etat membre.

Les autorités de contrôle coopèrent entre elles dans la mesure nécessaire à l'accomplissement de leurs missions, notamment en échangeant toute information utile.

7. Les Etats membres prévoient que les membres et agents des autorités de contrôle sont soumis, y compris après cessation de leurs activités, à l'obligation du secret professionnel à l'égard des informations confidentielles auxquelles ils ont accès.

Art. 29. Groupe de protection des personnes à l'égard du traitement des données à caractère personnel

1. Il est institué un groupe de protection des personnes à l'égard du traitement des données à caractère personnel, ci-après dénommé «groupe».

Le groupe a un caractère consultatif et indépendant.

2. Le groupe se compose d'un représentant de l'autorité ou des autorités de contrôle désignées par chaque Etat membre, d'un représentant de l'autorité ou des autorités créées pour les institutions et organismes communautaires et d'un représentant de la Commission.

Chaque membre du groupe est désigné par l'institution, l'autorité ou les autorités qu'il représente. Lorsqu'un Etat membre a désigné plusieurs autorités de contrôle, celles-ci procèdent à la nomination d'un représentant commun. Il en va de même pour les autorités créées pour les institutions et organismes communautaires.

3. Le groupe prend ses décisions à la majorité simple des représentants des autorités de contrôle.

4. Le groupe élit son président. La durée du mandat du président est de deux ans. Le mandat est renouvelable.

5. Le secrétariat du groupe est assuré par la Commission.

6. Le groupe établit son règlement intérieur.

7. Le groupe examine les questions mises à l'ordre du jour par son président, soit à l'initiative de celui-ci, soit à la demande d'un représentant des autorités de contrôle ou de la Commission.

Art. 30.

1. Le groupe a pour mission:

- a) d'examiner toute question portant sur la mise en oeuvre des dispositions nationales prises en application de la présente directive, en vue de contribuer à leur mise en oeuvre homogène;
- b) de donner à la Commission un avis sur le niveau de protection dans la Communauté et dans les pays tiers;
- c) de conseiller la Commission sur tout projet de modification de la présente directive, sur tout projet de mesures additionnelles ou spécifiques à prendre pour sauvegarder les droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel, ainsi que sur tout autre projet de mesures communautaires ayant une incidence sur ces droits et libertés;
- d) de donner un avis sur les codes de conduite élaborés au niveau communautaire.

2. Si le groupe constate que des divergences, susceptibles de porter atteinte à l'équivalence de la protection des personnes à l'égard du traitement des données à caractère personnel dans la Communauté, s'établissent entre les législations et pratiques des Etats membres, il en informe la Commission.

3. Le groupe peut émettre de sa propre initiative des recommandations sur toute question concernant la protection des personnes à l'égard du traitement de données à caractère personnel dans la Communauté.

4. Les avis et recommandations du groupe sont transmis à la Commission et au comité visé à l'article 31.

5. La Commission informe le groupe des suites qu'elle a données à ses avis et recommandations. Elle rédige à cet effet un rapport qui est transmis également au Parlement européen et au Conseil. Ce rapport est publié.

6. Le groupe établit un rapport annuel sur l'état de la protection des personnes physiques à l'égard du traitement des données à caractère personnel dans la Communauté et dans les pays tiers, qu'il communique à la Commission, au Parlement européen et au Conseil. Ce rapport est publié.

Chapitre VII. - Mesures d'exécution communautaires

Art. 31. Comité

1. La Commission est assistée par un comité composé des représentants des Etats membres et présidé par le représentant de la Commission.

2. Le représentant de la Commission soumet au comité un projet des mesures à prendre. Le comité émet son avis sur ce projet, dans un délai que le président peut fixer en fonction de l'urgence de la question en cause.

L'avis est émis à la majorité prévue à l'article 148 paragraphe 2 du traité. Lors des votes au sein du comité, les voix des représentants des Etats membres sont affectées de la pondération définie à l'article précité. Le président ne prend pas part au vote.

La Commission arrête des mesures qui sont immédiatement applicables. Toutefois, si elles ne sont pas conformes à l'avis émis par le comité, ces mesures sont aussitôt communiquées par la Commission au Conseil. Dans ce cas:

- la Commission diffère l'application des mesures décidées par elle d'un délai de trois mois à compter de la date de la communication,
- le Conseil, statuant à la majorité qualifiée, peut prendre une décision différente dans le délai prévu au premier tiret.

Dispositions finales

Art. 32.

1. Les Etats membres mettent en vigueur les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive au plus tard à l'issue d'une période de trois ans à compter de son adoption.

Lorsque les Etats membres adoptent ces dispositions, celles-ci contiennent une référence à la présente directive ou sont accompagnées d'une telle référence lors de leur publication officielle. Les modalités de cette référence sont arrêtées par les Etats membres.

2. Les Etats membres veillent à ce que les traitements dont la mise en oeuvre est antérieure à la date d'entrée en vigueur des dispositions nationales prises en application de la présente directive soient rendus conformes à ces dispositions au plus tard trois ans après cette date.

Par dérogation à l'alinéa précédent, les Etats membres peuvent prévoir que les traitements de données déjà contenues dans des fichiers manuels à la date d'entrée en vigueur des dispositions nationales prises en application de la présente directive seront rendus conformes aux articles 6, 7 et 8 de la présente directive dans un délai de douze ans à compter de la date d'adoption de celle-ci. Les Etats membres permettent toutefois à la personne concernée d'obtenir, à sa demande et notamment lors de l'exercice du droit d'accès, la rectification, l'effacement ou le verrouillage des données incomplètes, inexactes ou conservées d'une manière qui est incompatible avec les fins légitimes poursuivies par le responsable du traitement.

3. Par dérogation au paragraphe 2, les Etats membres peuvent prévoir, sous réserve des garanties appropriées, que les données conservées dans le seul but de la recherche historique ne soient pas rendues conformes aux articles 6, 7 et 8 de la présente directive.

4. Les Etats membres communiquent à la Commission le texte des dispositions de droit interne qu'ils adoptent dans le domaine régi par la présente directive.

Art. 33.

Périodiquement, et pour la première fois au plus tard trois ans après la date prévue à l'article 32 paragraphe 1^{er}, la Commission fait un rapport au Parlement européen et au Conseil sur l'application de la présente directive et l'assortit, le cas échéant, des propositions de modification appropriées. Ce rapport est publié.

La Commission examine, en particulier, l'application de la présente directive aux traitements de données constituées par des sons et des images, relatives aux personnes physiques, et elle présente les propositions appropriées qui pourraient s'avérer nécessaires en tenant compte des développements de la technologie de l'information et à la lumière de l'état des travaux sur la société de l'information.

Art. 34.

Les Etats membres sont destinataires de la présente directive.

Directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

(JOCE L - 201 du 31 juillet 2002, p. 37)

Le parlement européen et le conseil de l'union européenne,
vu le traité instituant la Communauté européenne, et notamment son article 95,
vu la proposition de la Commission¹,
vu l'avis du Comité économique et social²,
après consultation du Comité des régions,
statuant conformément à la procédure visée à l'article 251 du traité³,
considérant ce qui suit:

(1) La directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données⁴ exige que les Etats membres protègent les droits et les libertés des personnes physiques à l'égard du traitement des données à caractère personnel, et notamment le droit au respect de leur vie privée, afin d'assurer la libre circulation des données à caractère personnel dans la Communauté.

(2) La présente directive vise à respecter les droits fondamentaux et observe les principes reconnus notamment par la charte des droits fondamentaux de l'Union européenne. En particulier, elle vise à garantir le plein respect des droits exposés aux articles 7 et 8 de cette charte.

(3) La confidentialité des communications est garantie en conformité avec les instruments internationaux relatifs aux droits de l'homme, notamment la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et les constitutions des Etats membres.

(4) La directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications⁵ a traduit les principes définis dans la directive 95/46/CE en règles spécifiques applicables au secteur des télécommunications. La directive 97/66/CE doit être adaptée à l'évolution des marchés et des technologies des services de communications électroniques afin de garantir un niveau égal de protection des données à caractère personnel et de la vie privée aux utilisateurs de services de communications électroniques accessibles au public, indépendamment des technologies utilisées. Il convient, par conséquent, que ladite directive soit abrogée et remplacée par la présente directive.

(5) De nouvelles technologies numériques avancées qui posent des exigences spécifiques concernant la protection des données à caractère personnel et de la vie privée des utilisateurs sont actuellement introduites dans les réseaux publics de communications de la Communauté. Le développement de la société de l'information se caractérise par l'introduction de nouveaux services de communications électroniques. L'accès aux réseaux mobiles numériques s'est ouvert à un large public, à des conditions abordables. Ces réseaux numériques offrent de grandes capacités et de vastes possibilités pour le traitement des données à caractère personnel. Le succès du développement transfrontalier de ces services dépend en partie de la confiance qu'auront les utilisateurs que ces services ne porteront pas atteinte à leur vie privée.

(6) L'Internet bouleverse les structures commerciales traditionnelles en offrant une infrastructure mondiale commune pour la fourniture de toute une série de services de communications électroniques. Les services de communications électroniques accessibles au public sur l'Internet ouvrent de nouvelles possibilités aux utilisateurs, mais présentent aussi de nouveaux dangers pour leurs données à caractère personnel et leur vie privée.

(7) Dans le cas des réseaux publics de communications, il convient d'adopter des dispositions législatives, réglementaires et techniques spécifiques afin de protéger les droits et les libertés fondamentaux des personnes physiques et les intérêts légitimes des personnes morales, notamment eu égard à la capacité accrue de stockage et de traitement automatisés de données relatives aux abonnés et aux utilisateurs.

¹ JO C 365 E du 19.12.2000, p. 223.

² JO C 123 du 25.4.2001, p. 53.

³ Avis du Parlement européen du 13 novembre 2001 (non encore paru au Journal officiel), position commune du Conseil du 28 janvier 2002 (JO C 113 E du 14.5.2002, p. 39) et décision du Parlement européen du 30 mai 2002 (non encore parue au Journal officiel).
Décision du Conseil du 25 juin 2002.

⁴ JO L 281 du 23.11.1995, p. 31.

⁵ JO L 24 du 30.1.1998, p. 1.

(8) Il convient d'harmoniser les dispositions législatives, réglementaires et techniques adoptées par les Etats membres en ce qui concerne la protection des données à caractère personnel, de la vie privée et des intérêts légitimes des personnes morales dans le secteur des communications électroniques afin d'éviter de créer des obstacles au marché intérieur des communications électroniques conformément à l'article 14 du traité. L'harmonisation devrait être limitée aux exigences nécessaires pour garantir que la promotion et le développement de nouveaux services et réseaux de communications électroniques entre Etats membres ne sont pas entravés.

(9) Les Etats membres, les fournisseurs et les utilisateurs concernés, ainsi que les institutions communautaires compétentes, devraient coopérer à la conception et au développement des technologies pertinentes lorsque cela est nécessaire pour mettre en oeuvre les garanties prévues par la présente directive, en tenant particulièrement compte des objectifs qui consistent à réduire au minimum le traitement des données à caractère personnel et à utiliser des données anonymes ou pseudonymes lorsque c'est possible.

(10) Dans le secteur des communications électroniques, la directive 95/46/CE est applicable notamment à tous les aspects de la protection des droits et libertés fondamentaux qui n'entrent pas expressément dans le cadre de la présente directive, y compris les obligations auxquelles est soumis le responsable du traitement des données à caractère personnel et les droits individuels. La directive 95/46/CE s'applique aux services de communications électroniques non publics.

(11) À l'instar de la directive 95/46/CE, la présente directive ne traite pas des questions de protection des droits et libertés fondamentaux liées à des activités qui ne sont pas régies par le droit communautaire. Elle ne modifie donc pas l'équilibre existant entre le droit des personnes à une vie privée et la possibilité dont disposent les Etats membres de prendre des mesures telles que celles visées à l'article 15, paragraphe 1, de la présente directive, nécessaires pour la protection de la sécurité publique, de la défense, de la sûreté de l'Etat (y compris la prospérité économique de l'Etat lorsqu'il s'agit d'activités liées à la sûreté de l'Etat) et de l'application du droit pénal. Par conséquent, la présente directive ne porte pas atteinte à la faculté des Etats membres de procéder aux interceptions légales des communications électroniques ou d'arrêter d'autres mesures si cela s'avère nécessaire pour atteindre l'un quelconque des buts précités, dans le respect de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, telle qu'interprétée par la Cour européenne des droits de l'homme dans ses arrêts. Lesdites mesures doivent être appropriées, rigoureusement proportionnées au but poursuivi et nécessaires dans une société démocratique. Elles devraient également être subordonnées à des garanties appropriées, dans le respect de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

(12) Les abonnés à un service de communications électroniques accessible au public peuvent être des personnes physiques ou des personnes morales. En complétant la directive 95/46/CE, la présente directive vise à protéger les droits fondamentaux des personnes physiques et en particulier le droit au respect de leur vie privée, ainsi que les intérêts légitimes des personnes morales. La présente directive ne comporte aucune obligation pour les Etats membres d'étendre l'application de la directive 95/46/CE à la protection des intérêts légitimes des personnes morales, qui est garantie dans le cadre de la législation communautaire et nationale en vigueur.

(13) La relation contractuelle entre un abonné et un fournisseur de services peut prévoir un paiement périodique ou un versement unique pour le service fourni ou à fournir. Les cartes de prépaiement sont également considérées comme un contrat.

(14) Par «données de localisation», on peut entendre la latitude, la longitude et l'altitude du lieu où se trouve l'équipement terminal de l'utilisateur, la direction du mouvement, le degré de précision quant aux informations sur la localisation, l'identification de la cellule du réseau où se situe, à un moment donné, l'équipement terminal, ou encore le moment auquel l'information sur la localisation a été enregistrée.

(15) Une communication peut inclure toute information consistant en une dénomination, un nombre ou une adresse, fournie par celui qui émet la communication ou celui qui utilise une connexion pour effectuer la communication. Les données relatives au trafic peuvent inclure toute traduction de telles informations effectuée par le réseau par lequel la communication est transmise en vue d'effectuer la transmission. Les données relatives au trafic peuvent, entre autres, comporter des données concernant le routage, la durée, le moment ou le volume d'une communication, le protocole de référence, l'emplacement des équipements terminaux de l'expéditeur ou du destinataire, le réseau de départ ou d'arrivée de la communication, ou encore le début, la fin ou la durée d'une connexion. Elles peuvent également représenter le format dans lequel la communication a été acheminée par le réseau.

(16) Les informations qui font partie d'un service de radiodiffusion fourni sur un réseau public de communications le sont à l'intention d'un nombre virtuellement illimité d'auditeurs et/ou de téléspectateurs et ne constituent pas une communication au sens de la présente directive. Par contre, lorsqu'il est possible

d'identifier l'abonné ou utilisateur individuel qui reçoit ces informations, comme, par exemple, dans le cas de la fourniture de services vidéo à la demande, les informations acheminées s'inscrivent dans la définition de «communication» au sens de la présente directive.

(17) Aux fins de la présente directive, le consentement d'un utilisateur ou d'un abonné, que ce dernier soit une personne physique ou morale, devrait avoir le même sens que le consentement de la personne concernée tel que défini et précisé davantage par la directive 95/46/CE. Le consentement peut être donné selon toute modalité appropriée permettant à l'utilisateur d'indiquer ses souhaits librement, de manière spécifique et informée, y compris en cochant une case lorsqu'il visite un site Internet.

(18) Les services à valeur ajoutée peuvent, par exemple, comprendre des conseils sur les forfaits tarifaires les plus avantageux ou sur le guidage routier, des informations sur l'état de la circulation, des prévisions météorologiques ou des informations touristiques.

(19) L'application de certaines exigences relatives à la présentation et à la restriction de l'identification des lignes appelante et connectée et au renvoi d'appel automatique vers des lignes d'abonné connectées à des centraux analogiques ne devrait pas être rendue obligatoire dans les cas spécifiques où une telle application s'avérerait techniquement impossible ou exigerait un effort économique disproportionné. Il est important que les parties intéressées soient informées de ces cas et les Etats membres devraient donc les communiquer à la Commission.

(20) Il convient que les fournisseurs de services prennent les mesures appropriées pour assurer la sécurité de leurs services, le cas échéant conjointement avec le fournisseur du réseau, et informent les abonnés des risques particuliers liés à une violation de la sécurité du réseau. De tels risques peuvent notamment toucher les services de communications électroniques fournis par l'intermédiaire d'un réseau ouvert tel que l'Internet ou la téléphonie mobile analogique. Il est particulièrement important que les abonnés et les utilisateurs de ces services soient pleinement informés par leur fournisseur de service des risques existants en matière de sécurité contre lesquels ce dernier est dépourvu de moyens d'action. Il convient que les fournisseurs de services qui proposent des services de communications électroniques accessibles au public sur l'Internet informent les utilisateurs et les abonnés des mesures qu'ils peuvent prendre pour sécuriser leurs communications, par exemple en recourant à des types spécifiques de logiciels ou de techniques de cryptage. L'obligation qui est faite à un fournisseur de service d'informer les abonnés de certains risques en matière de sécurité ne le dispense pas de prendre immédiatement les mesures appropriées pour remédier à tout nouveau risque imprévisible en matière de sécurité et rétablir le niveau normal de sécurité du service, les frais en étant à sa seule charge. L'information de l'abonné sur les risques en matière de sécurité devrait être gratuite, excepté les frais nominaux qu'un abonné peut être amené à supporter lorsqu'il reçoit ou collecte des informations, par exemple en téléchargeant un message reçu par courrier électronique. La sécurité s'apprécie au regard de l'article 17 de la directive 95/46/CE.

(21) Il convient de prendre des mesures pour empêcher tout accès non autorisé aux communications afin de protéger la confidentialité des communications effectuées au moyen de réseaux publics de communications et de services de communications électroniques accessibles au public, y compris de leur contenu et de toute donnée afférente à ces communications. La législation nationale de certains Etats membres interdit uniquement l'accès non autorisé intentionnel aux communications.

(22) L'interdiction du stockage des communications et des données relatives au trafic y afférentes par des personnes autres que les utilisateurs ou sans le consentement de ceux-ci ne vise pas à interdire tout stockage automatique, intermédiaire et transitoire de ces informations si ce stockage a lieu dans le seul but d'effectuer la transmission dans le réseau de communications électroniques, pour autant que les informations ne soient pas stockées pour une durée plus longue que le temps nécessaire à la transmission et à la gestion du trafic et qu'au cours de la période de stockage la confidentialité des informations reste garantie. Dans la mesure où l'exige la transmission plus efficace d'informations accessibles au public à d'autres destinataires du service à leur demande, la présente directive ne fait pas obstacle à ce que ces informations soient stockées plus longtemps, à condition qu'elles soient accessibles au public en tout état de cause et sans aucune restriction et que toute donnée concernant les abonnés ou utilisateurs individuels qui les demandent soit effacée.

(23) La confidentialité des communications devrait également être assurée dans les transactions commerciales licites. Au besoin et sous réserve d'une autorisation légale, les communications peuvent être enregistrées pour servir de preuve d'une transaction commerciale. La directive 95/46/CE est applicable en pareil cas. Les parties aux communications devraient être informées de l'enregistrement avant qu'il n'ait lieu, de la ou des raisons pour lesquelles la communication est enregistrée et de la durée du stockage de l'enregistrement. La communication enregistrée devrait être effacée dès que possible et, en tout état de cause, lors de l'expiration du délai légal de recours contre la transaction.

(24) L'équipement terminal de l'utilisateur d'un réseau de communications électroniques ainsi que toute information stockée sur cet équipement relèvent de la vie privée de l'utilisateur, qui doit être protégée au titre de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. Or, les logiciels espions, les pixels invisibles (web bugs), les identificateurs cachés et les autres dispositifs analogues peuvent pénétrer dans le terminal de l'utilisateur à son insu afin de pouvoir accéder à des informations, stocker des informations cachées ou suivre les activités de l'utilisateur, et peuvent porter gravement atteinte à la vie privée de ce dernier. L'utilisation de tels dispositifs ne devrait être autorisée qu'à des fins légitimes, et en étant portée à la connaissance de l'utilisateur concerné.

(25) Cependant, les dispositifs de ce type, par exemple des témoins de connexion (cookies), peuvent constituer un outil légitime et utile, par exemple pour évaluer l'efficacité de la conception d'un site et de la publicité faite pour ce site, ainsi que pour contrôler l'identité des utilisateurs effectuant des transactions en ligne. Lorsque des dispositifs du type précité, tels que des témoins de connexion, sont destinés à des fins légitimes, par exemple faciliter la fourniture de services de la société de l'information, leur utilisation devrait être autorisée à condition que les utilisateurs se voient donner des informations claires et précises, conformément à la directive 95/46/CE, sur la finalité des témoins de connexion ou des dispositifs analogues de manière à être au courant des informations placées sur l'équipement terminal qu'ils utilisent. Les utilisateurs devraient avoir la possibilité de refuser qu'un témoin de connexion ou un dispositif similaire soit placé sur leur équipement terminal. Ce point est particulièrement important pour les cas où des utilisateurs autres que l'utilisateur original ont accès à l'équipement terminal et donc aux données sensibles à caractère privé qui y sont stockées. L'information relative à l'utilisation de plusieurs dispositifs à installer sur l'équipement terminal de l'utilisateur ainsi que le droit de refuser ces dispositifs peuvent être offerts en une seule fois pendant une même connexion, et couvrir aussi l'utilisation future qui pourrait être faite de ces dispositifs durant des connexions subséquentes. Les méthodes retenues pour communiquer des informations, offrir un droit de refus ou solliciter le consentement devraient être les plus conviviales possibles. L'accès au contenu d'un site spécifique peut être, toutefois, subordonné au fait d'accepter, en pleine connaissance de cause, l'installation d'un témoin de connexion ou d'un dispositif analogue, si celui-ci est utilisé à des fins légitimes.

(26) Les données relatives aux abonnés qui sont traitées dans des réseaux de communications électroniques pour établir des connexions et transmettre des informations contiennent des informations sur la vie privée des personnes physiques et touchent au droit au secret de leur correspondance ainsi qu'aux intérêts légitimes des personnes morales. Ces données ne peuvent être stockées que dans la mesure où cela est nécessaire à la fourniture du service, aux fins de la facturation et des paiements pour interconnexion, et ce, pour une durée limitée. Tout autre traitement de ces données que le fournisseur du service de communications électroniques accessible au public peut vouloir effectuer pour la commercialisation des services de communications électroniques ou pour la fourniture de services à valeur ajoutée ne peut être autorisé que si l'abonné a donné son accord sur la base d'informations précises et complètes fournies par le fournisseur du service de communications électroniques accessible au public sur la nature des autres traitements qu'il envisage d'effectuer, ainsi que sur le droit de l'abonné de ne pas donner son consentement à ces traitements ou de retirer son consentement. Il convient également d'effacer ou de rendre anonymes les données relatives au trafic utilisées pour la commercialisation de services de communications ou pour la fourniture de services à valeur ajoutée, lorsque les services en question ont été fournis. Il convient que les fournisseurs de services tiennent toujours leurs abonnés informés des types de données qu'ils traitent, des finalités de ces traitements et de leur durée.

(27) Le moment exact où s'achève la transmission d'une communication, au-delà duquel les données relatives au trafic doivent être effacées sauf à des fins de facturation, peut dépendre du type de service de communications électroniques fourni. Ainsi, dans le cas d'un appel par téléphonie vocale, la transmission cesse dès que l'un ou l'autre des usagers interrompt la connexion et, dans le cas d'un courrier électronique, la transmission prend fin dès que le destinataire récupère le message, généralement à partir du serveur de son fournisseur de service.

(28) L'obligation d'effacer ou de rendre anonymes les données relatives au trafic lorsqu'elles ne sont plus nécessaires aux fins de la transmission d'une communication n'est pas contradictoire avec les procédures utilisées sur l'Internet, telles que celle de la mise en antémémoire (caching), dans le système des noms de domaines, pour les adresses IP ou pour les liens entre une adresse IP et une adresse physique, ou l'utilisation d'informations relatives à la connexion pour contrôler le droit d'accès à des réseaux ou à des services.

(29) Au besoin, et au cas par cas, le fournisseur d'un service peut traiter des données relatives au trafic qui concernent des abonnés ou des utilisateurs s'il s'agit de déceler une défaillance technique ou une erreur dans la transmission des communications. Des données relatives au trafic nécessaires pour la facturation peuvent aussi être traitées par le fournisseur d'un service s'il s'agit de déceler et de faire cesser des pratiques frauduleuses consistant à utiliser le service de communications électroniques sans le payer.

(30) Les systèmes mis au point pour la fourniture de réseaux et de services de communications électroniques devraient être conçus de manière à limiter au strict minimum la quantité de données personnelles nécessaires. Toute activité qui s'inscrit dans le cadre de la fourniture d'un service de communications électroniques et qui va au-delà de la simple transmission d'une communication ou de sa facturation devrait se fonder sur des données relatives au trafic globalisées qui ne peuvent pas être attribuées à des abonnés ou utilisateurs individuels. Si cette activité ne peut se fonder sur des données globalisées, elle devrait être considérée comme un service à valeur ajoutée, pour lequel le consentement de l'abonné est nécessaire.

(31) La question de savoir si c'est de l'utilisateur ou de l'abonné qu'il convient d'obtenir le consentement pour pouvoir traiter des données à caractère personnel en vue de fournir un service donné à valeur ajoutée sera fonction des données à traiter et du type de service à fournir mais aussi de la possibilité ou non, sur les plans technique, procédural et contractuel, de distinguer le particulier qui utilise un service de communications électroniques de la personne, physique ou morale, qui s'y est abonnée.

(32) Lorsque le fournisseur d'un service de communications électroniques ou d'un service à valeur ajoutée fait sous-traiter le traitement des données à caractère personnel nécessaires à la fourniture desdits services, cette sous-traitance et le traitement des données qui en découle devraient respecter intégralement les exigences de la directive 95/46/CE pour ce qui est des responsables du contrôle et du traitement des données à caractère personnel. Lorsque, pour permettre la fourniture d'un service à valeur ajoutée, des données relatives au trafic ou à la localisation sont transmises par un fournisseur de services de communications électroniques à un fournisseur de services à valeur ajoutée, les abonnés ou utilisateurs auxquels ces données se rapportent devraient également être pleinement informés de cette transmission avant de consentir ou non au traitement desdites données.

(33) L'introduction de factures détaillées a amélioré les possibilités offertes à l'abonné pour vérifier l'exactitude des montants facturés par le fournisseur de service mais elle risque simultanément de compromettre la vie privée des utilisateurs de services de communications électroniques accessibles au public. Par conséquent, pour protéger la vie privée des utilisateurs, les Etats membres devraient encourager la mise au point, dans le domaine des services de communications électroniques, d'options telles que de nouvelles formules de paiement permettant d'accéder de manière anonyme ou strictement privée aux services de communications électroniques accessibles au public, par exemple des télécartes et des facilités de paiement par carte de crédit. Aux mêmes fins, les Etats membres peuvent inviter les opérateurs à proposer à leurs abonnés un autre type de facture détaillée sur laquelle un certain nombre de chiffres des numéros d'appel ont été supprimés.

(34) Il est nécessaire, en ce qui concerne l'identification de la ligne appelante, de protéger le droit qu'a l'auteur d'un appel d'empêcher la présentation de l'identification de la ligne à partir de laquelle l'appel est effectué, ainsi que le droit de la personne appelée de refuser les appels provenant de lignes non identifiées. Dans des cas spécifiques, il est justifié d'empêcher que la présentation de l'identification de la ligne appelante soit supprimée. Certains abonnés, en particulier les services d'assistance téléphoniques et les autres organismes similaires, ont intérêt à garantir l'anonymat de ceux qui les appellent. Il est nécessaire, en ce qui concerne l'identification de la ligne connectée, de protéger le droit et l'intérêt légitime qu'a la personne appelée d'empêcher la présentation de l'identification de la ligne à laquelle l'auteur de l'appel est effectivement connecté, en particulier dans le cas d'appels renvoyés. Il convient que les fournisseurs de services de communications électroniques accessibles au public informent leurs abonnés de l'existence, sur le réseau, de l'identification des lignes appelante et connectée, ainsi que de tous les services offerts sur la base de l'identification des lignes appelante et connectée et des possibilités offertes en matière de protection de la vie privée. Cela permettra aux abonnés de choisir en connaissance de cause, parmi les possibilités qui leur sont offertes en matière de protection de la vie privée, celles dont ils souhaiteraient faire usage. Les possibilités qui sont offertes en matière de protection de la vie privée pour chaque ligne ne doivent pas nécessairement être disponibles comme un service automatique du réseau, mais peuvent être obtenues sur simple demande auprès du fournisseur du service de communications électroniques accessible au public.

(35) Dans les réseaux de communications mobiles, des données de localisation indiquant la position géographique de l'équipement terminal de l'utilisateur mobile sont traitées afin de permettre la transmission des communications. Ces données sont des données relatives au trafic couvertes par l'article 6 de la présente directive. Toutefois, les réseaux numériques mobiles peuvent aussi avoir la capacité de traiter des données de localisation qui sont plus précises que ne l'exige la transmission des communications et qui sont utilisées pour la fourniture de services à valeur ajoutée tels que des services personnalisés d'information sur la circulation et de guidage des conducteurs. Le traitement de ces données en vue de la fourniture de services à valeur ajoutée ne devrait être autorisé que lorsque les abonnés ont donné leur consentement. Même dans ce cas, les abonnés devraient disposer d'un moyen simple pour interdire temporairement le traitement des données de localisation et ce, gratuitement.

(36) Les Etats membres peuvent prévoir une limitation du droit de l'utilisateur ou de l'abonné à la vie privée en ce qui concerne l'identification de la ligne appelante lorsque cela est nécessaire pour déterminer l'origine des appels malveillants et en ce qui concerne les données d'identification et de localisation de la ligne appelante lorsque cela est nécessaire pour permettre aux services d'urgence d'intervenir le plus efficacement possible. À ces fins, les Etats membres peuvent adopter des mesures spécifiques autorisant les fournisseurs de services de communications électroniques à mettre à disposition les données d'identification et de localisation de la ligne appelante sans le contentement préalable de l'utilisateur ou de l'abonné concerné.

(37) Il importe de protéger les abonnés contre toute gêne que pourrait leur causer le renvoi automatique d'appels par d'autres personnes. En outre, en pareil cas, les abonnés doivent pouvoir faire cesser le transfert des appels renvoyés sur leurs terminaux sur simple demande adressée au fournisseur du service de communications électroniques accessible au public.

(38) Les annuaires d'abonnés aux services de communications électroniques sont largement diffusés et publics. Pour protéger la vie privée des personnes physiques et l'intérêt légitime des personnes morales, il importe que l'abonné soit à même de déterminer si les données à caractère personnel qui le concernent doivent être publiées dans un annuaire et, dans l'affirmative, lesquelles de ces données doivent être rendues publiques. Il convient que les fournisseurs d'annuaires publics informent les abonnés qui figureront dans ces annuaires des fins auxquelles ceux-ci sont établis et de toute utilisation particulière qui peut être faite des versions électroniques des annuaires publics, notamment grâce aux fonctions de recherche intégrées dans le logiciel, telles que les fonctions de recherche inverse qui permettent aux utilisateurs d'un annuaire de trouver le nom et l'adresse d'un abonné à partir d'un simple numéro de téléphone.

(39) C'est à la partie qui collecte des données à caractère personnel auprès d'abonnés que devrait incomber l'obligation d'informer ceux-ci des fins auxquelles sont établis des annuaires publics comportant des données personnelles les concernant. Si ces données peuvent être transmises à un ou plusieurs tiers, l'abonné devrait être informé de cette possibilité ainsi que des destinataires ou catégories de destinataires éventuels. Une telle transmission ne devrait pouvoir se faire que s'il est garanti que les données ne pourront pas être utilisées à des fins autres que celles pour lesquelles elles ont été collectées. Si la partie qui a collecté ces données auprès de l'abonné ou un tiers quelconque auquel elles ont été transmises souhaitent les exploiter à d'autres fins, ladite partie ou ledit tiers devront obtenir une nouvelle fois le consentement de l'abonné.

(40) Il importe de protéger les abonnés contre toute violation de leur vie privée par des communications non sollicitées effectuées à des fins de prospection directe, en particulier au moyen d'automates d'appel, de télécopies et de courriers électroniques, y compris les messages courts (SMS). Si ces formes de communications commerciales non sollicitées peuvent être relativement faciles et peu onéreuses à envoyer, elles peuvent, en revanche imposer une charge et/ou un coût à leur destinataire. En outre, dans certains cas, leur volume peut poser un problème pour les réseaux de communications électroniques et les équipements terminaux. S'agissant de ces formes de communications non sollicitées effectuées à des fins de prospection directe, il est justifié d'exiger de l'expéditeur qu'il ait obtenu le consentement préalable du destinataire avant de les lui envoyer. Le marché unique exige une approche harmonisée à cet égard afin que les entreprises comme les utilisateurs disposent de règles simples s'appliquant à l'échelle de la Communauté.

(41) Dans le cadre d'une relation client-fournisseur existante, il est raisonnable d'autoriser l'entreprise qui, conformément à la directive 95/46/CE, a obtenu les coordonnées électroniques, et exclusivement celle-ci, à exploiter ces coordonnées électroniques pour proposer au client des produits ou des services similaires. Il conviendrait, lorsque des coordonnées électroniques sont recueillies, que le client soit informé clairement et distinctement sur leur utilisation ultérieure à des fins de prospection directe et qu'il lui soit donné la faculté de s'opposer à cet usage. Il convient de continuer d'offrir cette possibilité lors de chaque message de prospection directe ultérieur, et ce, sans frais, hormis les coûts liés à la transmission du refus.

(42) Il existe d'autres formes de prospection directe qui sont plus onéreuses pour l'expéditeur et n'imposent aucune charge financière à l'abonné ou à l'utilisateur, tels que les appels téléphoniques personnels, et qui pourraient justifier l'établissement d'un système permettant aux abonnés et aux utilisateurs d'indiquer qu'ils ne souhaitent pas recevoir de tels appels. Afin de ne pas abaisser les niveaux existants de protection de la vie privée, il conviendrait néanmoins que les Etats membres soient autorisés à maintenir en vigueur les systèmes nationaux et à n'autoriser que les appels destinés à des abonnés ou utilisateurs qui ont donné leur consentement préalable.

(43) Afin de faciliter la mise en oeuvre effective des règles communautaires relatives aux messages de prospection directe non sollicités, il importe d'interdire d'émettre des messages non sollicités à des fins de prospection directe sous une fausse identité, une fausse adresse de réponse ou un faux numéro.

(44) Certains systèmes de messagerie électronique permettent aux abonnés de visualiser le nom de l'expéditeur et l'objet d'un message électronique, ainsi que d'effacer le message sans devoir télécharger le reste du contenu dudit message ou d'une quelconque pièce jointe, ce qui réduit les coûts que pourrait engendrer le téléchargement d'un courrier électronique non sollicité ou d'une de ses pièces jointes. Dans certains cas, de telles modalités peuvent continuer de s'avérer utiles en tant qu'outil complémentaire des exigences générales énoncées par la présente directive.

(45) La présente directive est sans préjudice des dispositions que les Etats membres prennent pour protéger les intérêts légitimes des personnes morales à l'égard des communications non sollicitées à des fins de prospection directe. Lorsque les Etats membres établissent un registre opt-out pour les communications en question adressées aux personnes morales, essentiellement des utilisateurs professionnels, les dispositions de l'article 7 de la directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (directive sur le commerce électronique)¹ s'appliquent pleinement.

(46) Les fonctionnalités permettant la fourniture de services de communications électroniques peuvent être intégrées dans le réseau ou dans tout élément de l'équipement terminal de l'utilisateur, y compris le logiciel. La protection des données à caractère personnel et de la vie privée de l'utilisateur de services de communications électroniques accessibles au public devrait être indépendante de la configuration des différents éléments nécessaires à la fourniture du service et de la répartition des fonctionnalités requises entre ces éléments. La directive 95/46/CE s'applique à toute forme de traitement de données à caractère personnel, quelle que soit la technologie utilisée. L'existence de règles spécifiques aux services de communications électroniques parallèlement à des règles générales s'appliquant aux autres éléments nécessaires à la fourniture de ces services peut ne pas faciliter la protection des données à caractère personnel et de la vie privée d'une manière technologiquement neutre. Il peut, par conséquent, être nécessaire d'adopter des mesures exigeant que les fabricants de certains types d'équipements utilisés pour les services de communications électroniques intègrent dans leurs produits des sauvegardes afin d'assurer la protection des données à caractère personnel et de la vie privée des utilisateurs et des abonnés. L'adoption de telles mesures conformément à la directive 1999/5/CE du Parlement européen et du Conseil du 9 mars 1999 concernant les équipements hertziens et les équipements terminaux de télécommunications et la reconnaissance mutuelle de leur conformité² garantira que l'introduction de certaines caractéristiques techniques des équipements de communications électroniques, y compris des logiciels, en vue d'assurer la protection des données soit harmonisée pour être compatible avec la mise en oeuvre du marché intérieur.

(47) Lorsque les droits des utilisateurs et des abonnés ne sont pas respectés, il convient que la législation nationale prévoie des recours juridictionnels. Des sanctions devraient être infligées à toute personne, qu'elle relève du droit privé ou du droit public, qui ne respecte pas les mesures nationales prises en vertu de la présente directive.

(48) Il est utile, dans le champ d'application de la présente directive, de tirer parti de l'expérience acquise par le groupe de protection des personnes à l'égard du traitement des données à caractère personnel, composé de représentants des autorités de contrôle désignées par chaque Etat membre, institué par l'article 29 de la directive 95/46/CE.

(49) Afin de faciliter le respect de la présente directive, certaines dispositions spécifiques sont nécessaires pour le traitement des données en cours à la date d'entrée en vigueur des dispositions nationales transposant la présente directive dans le droit interne des Etats membres,

Ont arrêté la présente directive:

Art. 1^{er}. Champ d'application et objectif

1. La présente directive harmonise les dispositions des Etats membres nécessaires pour assurer un niveau équivalent de protection des droits et libertés fondamentaux, et en particulier du droit à la vie privée, en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques, ainsi que la libre circulation de ces données et des équipements et des services de communications électroniques dans la Communauté.

2. Les dispositions de la présente directive précisent et complètent la directive 95/46/CE aux fins énoncées au paragraphe 1^{er}. En outre, elles prévoient la protection des intérêts légitimes des abonnés qui sont des personnes morales.

¹ JO L 178 du 17.7.2000, p. 1.

² JO L 91 du 7.4.1999, p. 10.

3. La présente directive ne s'applique pas aux activités qui ne relèvent pas du traité instituant la Communauté européenne, telles que celles visées dans les titres V et VI du traité sur l'Union européenne, et, en tout état de cause, aux activités concernant la sécurité publique, la défense, la sûreté de l'Etat (y compris la prospérité économique de l'Etat lorsqu'il s'agit d'activités liées à la sûreté de l'Etat) ou aux activités de l'Etat dans des domaines relevant du droit pénal.

Art. 2. Définitions

Sauf disposition contraire, les définitions figurant dans la directive 95/46/CE et dans la directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et les services de communications électroniques (directive «cadre»)¹ s'appliquent aux fins de la présente directive.

Les définitions suivantes sont aussi applicables:

- a) «utilisateur»: toute personne physique utilisant un service de communications électroniques accessible au public à des fins privées ou professionnelles sans être nécessairement abonnée à ce service;
- b) «données relatives au trafic»: toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation;
- c) «données de localisation»: toutes les données traitées dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public;
- d) «communication»: toute information échangée ou acheminée entre un nombre fini de parties au moyen d'un service de communications électroniques accessible au public. Cela ne comprend pas les informations qui sont acheminées dans le cadre d'un service de radiodiffusion au public par l'intermédiaire d'un réseau de communications électroniques, sauf dans la mesure où un lien peut être établi entre l'information et l'abonné ou utilisateur identifiable qui la reçoit;
- e) «appel»: une connexion établie au moyen d'un service téléphonique accessible au public permettant une communication bidirectionnelle en temps réel;
- f) le «consentement» d'un utilisateur ou d'un abonné correspond au «consentement de la personne concernée» figurant dans la directive 95/46/CE;
- g) «service à valeur ajoutée»: tout service qui exige le traitement de données relatives au trafic ou à la localisation, à l'exclusion des données qui ne sont pas indispensables pour la transmission d'une communication ou sa facturation;
- h) «courrier électronique»: tout message sous forme de texte, de voix, de son ou d'image envoyé par un réseau public de communications qui peut être stocké dans le réseau ou dans l'équipement terminal du destinataire jusqu'à ce que ce dernier le récupère.

Art. 3. Services concernés

1. La présente directive s'applique au traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communications dans la Communauté.

2. Les articles 8, 10 et 11 s'appliquent aux lignes d'abonnés connectées à des centraux numériques et, lorsque cela est techniquement possible et ne nécessite pas un effort économique disproportionné, aux lignes d'abonnés connectées à des centraux analogiques.

3. Lorsqu'il est techniquement impossible de se conformer aux exigences des articles 8, 10 et 11 ou lorsque cela nécessite un effort économique disproportionné, les Etats membres en informent la Commission.

Art. 4. Sécurité

1. Le fournisseur d'un service de communications électroniques accessible au public prend les mesures d'ordre technique et organisationnel appropriées afin de garantir la sécurité de ses services, le cas échéant conjointement avec le fournisseur du réseau public de communications en ce qui concerne la sécurité du réseau. Compte tenu des possibilités techniques les plus récentes et du coût de leur mise en oeuvre, ces mesures garantissent un degré de sécurité adapté au risque existant.

2. Lorsqu'il existe un risque particulier de violation de la sécurité du réseau, le fournisseur d'un service de communications électroniques accessible au public informe les abonnés de ce risque et, si les mesures que peut prendre le fournisseur du service ne permettent pas de l'écarter, de tout moyen éventuel d'y remédier, y compris en en indiquant le coût probable.

¹ JO L 108 du 24.4.2002, p. 33.

Art. 5. Confidentialité des communications

1. Les Etats membres garantissent, par la législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes. En particulier, ils interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée, conformément à l'article 15, paragraphe 1. Le présent paragraphe n'empêche pas le stockage technique nécessaire à l'acheminement d'une communication, sans préjudice du principe de confidentialité.

2. Le paragraphe 1^{er} n'affecte pas l'enregistrement légalement autorisé de communications et des données relatives au trafic y afférentes, lorsqu'il est effectué dans le cadre des usages professionnels licites, afin de fournir la preuve d'une transaction commerciale ou de toute autre communication commerciale.

3. Les Etats membres garantissent que l'utilisation des réseaux de communications électroniques en vue de stocker des informations ou d'accéder à des informations stockées dans l'équipement terminal d'un abonné ou d'un utilisateur ne soit permise qu'à condition que l'abonné ou l'utilisateur, soit muni, dans le respect de la directive 95/46/CE, d'une information claire et complète, entre autres sur les finalités du traitement, et que l'abonné ou l'utilisateur ait le droit de refuser un tel traitement par le responsable du traitement des données. Cette disposition ne fait pas obstacle à un stockage ou à un accès techniques visant exclusivement à effectuer ou à faciliter la transmission d'une communication par la voie d'un réseau de communications électroniques, ou strictement nécessaires à la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur.

Art. 6. Données relatives au trafic

1. Les données relatives au trafic concernant les abonnés et les utilisateurs traitées et stockées par le fournisseur d'un réseau public de communications ou d'un service de communications électroniques accessibles au public doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication sans préjudice des paragraphes 2, 3 et 5, du présent article ainsi que de l'article 15, paragraphe 1^{er}.

2. Les données relatives au trafic qui sont nécessaires pour établir les factures des abonnés et les paiements pour interconnexion peuvent être traitées. Un tel traitement n'est autorisé que jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement.

3. Afin de commercialiser ses services de communications électroniques ou de fournir des services à valeur ajoutée, le fournisseur d'un service de communications électroniques accessible au public peut traiter les données visées au paragraphe 1^{er} dans la mesure et pour la durée nécessaires à la fourniture ou à la commercialisation de ces services, pour autant que l'abonné ou l'utilisateur que concernent ces données ait donné son consentement. Les utilisateurs ou abonnés ont la possibilité de retirer à tout moment leur consentement pour le traitement des données relatives au trafic.

4. Le fournisseur de service doit informer l'abonné ou l'utilisateur des types de données relatives au trafic qui sont traités ainsi que de la durée de ce traitement aux fins visées au paragraphe 2 et, avant d'obtenir leur consentement, aux fins visées au paragraphe 3.

5. Le traitement des données relatives au trafic effectué conformément aux dispositions des paragraphes 1, 2, 3 et 4 doit être restreint aux personnes agissant sous l'autorité des fournisseurs de réseaux publics de communications et de services de communications électroniques accessibles au public qui sont chargées d'assurer la facturation ou la gestion du trafic, de répondre aux demandes de la clientèle, de détecter les fraudes et de commercialiser les services de communications électroniques ou de fournir un service à valeur ajoutée; ce traitement doit se limiter à ce qui est nécessaire à de telles activités.

6. Les paragraphes 1, 2, 3 et 5 s'appliquent sans préjudice de la possibilité qu'ont les organes compétents de se faire communiquer des données relatives au trafic conformément à la législation en vigueur dans le but de régler des litiges, notamment en matière d'interconnexion ou de facturation.

Art. 7. Facturation détaillée

1. Les abonnés ont le droit de recevoir des factures non détaillées.

2. Les Etats membres appliquent des dispositions nationales afin de concilier les droits des abonnés recevant des factures détaillées avec le droit à la vie privée des utilisateurs appelants et des abonnés

appelés, par exemple en veillant à ce que lesdits utilisateurs et abonnés disposent de modalités complémentaires suffisantes renforçant le respect de la vie privée pour les communications ou les paiements.

Art. 8. Présentation et restriction de l'identification de la ligne appelante et de la ligne connectée

1. Dans les cas où la présentation de l'identification de la ligne appelante est offerte, le fournisseur du service doit offrir à l'utilisateur appelant, par un moyen simple et gratuit, la possibilité d'empêcher la présentation de l'identification de la ligne appelante, et ce, appel par appel. L'abonné appelant doit avoir cette possibilité pour chaque ligne.

2. Dans les cas où la présentation de l'identification de la ligne appelante est offerte, le fournisseur du service doit offrir à l'abonné appelé, par un moyen simple et gratuit pour un usage raisonnable de cette fonction, la possibilité d'empêcher la présentation de l'identification de la ligne appelante pour les appels entrants.

3. Dans les cas où la présentation de l'identification de la ligne appelante est offerte et où l'identification de la ligne appelante est présentée avant l'établissement de l'appel, le fournisseur de service doit offrir à l'abonné appelé, par un moyen simple, la possibilité de refuser les appels entrants lorsque l'utilisateur ou l'abonné appelant a empêché la présentation de l'identification de la ligne appelante.

4. Dans les cas où la présentation de l'identification de la ligne connectée est offerte, le fournisseur de service doit offrir à l'abonné appelé, par un moyen simple et gratuit, la possibilité d'empêcher la présentation de l'identification de la ligne connectée à l'utilisateur appelant.

5. Le paragraphe 1^{er} s'applique également aux appels provenant de la Communauté à destination de pays tiers. Les paragraphes 2, 3 et 4 s'appliquent également aux appels entrants provenant de pays tiers.

6. Les Etats membres veillent à ce que, dans les cas où la présentation de l'identification de la ligne appelante et/ou de la ligne connectée est offerte, les fournisseurs de services de communications électroniques accessibles au public informent le public de cette situation, ainsi que des possibilités prévues aux paragraphes 1, 2, 3 et 4.

Art. 9. Données de localisation autres que les données relatives au trafic

1. Lorsque des données de localisation, autres que des données relatives au trafic, concernant des utilisateurs ou abonnés de réseaux publics de communications ou de services de communications électroniques accessibles au public ou des abonnés à ces réseaux ou services, peuvent être traitées, elles ne le seront qu'après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés, dans la mesure et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée. Le fournisseur du service doit informer les utilisateurs ou les abonnés, avant d'obtenir leur consentement, du type de données de localisation autres que les données relatives au trafic qui sera traité, des objectifs et de la durée de ce traitement, et du fait que les données seront ou non transmises à un tiers en vue de la fourniture du service à valeur ajoutée. Les utilisateurs ou les abonnés ont la possibilité de retirer à tout moment leur consentement pour le traitement des données de localisation autres que les données relatives au trafic.

2. Lorsque les utilisateurs ou les abonnés ont donné leur consentement au traitement des données de localisation autres que les données relatives au trafic, ils doivent garder la possibilité d'interdire temporairement, par un moyen simple et gratuit, le traitement de ces données pour chaque connexion au réseau ou pour chaque transmission de communication.

3. Le traitement des données de localisation autres que les données relatives au trafic effectué conformément aux paragraphes 1 et 2 doit être restreint aux personnes agissant sous l'autorité du fournisseur du réseau public de communications ou service de communications électroniques accessible au public ou du tiers qui fournit le service à valeur ajoutée, et doit se limiter à ce qui est nécessaire pour assurer la fourniture du service à valeur ajoutée.

Art. 10. Dérogations

Les Etats membres veillent à ce que des procédures transparentes régissent les modalités grâce auxquelles le fournisseur d'un réseau public de communications ou d'un service de communications électroniques accessible au public peut passer outre:

- a) à la suppression de la présentation de l'identification de la ligne appelante, à titre temporaire, lorsqu'un abonné demande l'identification d'appels malveillants ou dérangeants; dans ce cas, conformément au droit interne, les données permettant d'identifier l'abonné appelant seront conservées et mises à disposition par le fournisseur d'un réseau public de communications et/ou d'un service de communications électroniques accessible au public;

b) à la suppression de la présentation de l'identification de la ligne appelante et à l'interdiction temporaire ou à l'absence de consentement d'un abonné ou d'un utilisateur en ce qui concerne le traitement de données de localisation, ligne par ligne, pour les organismes chargés de traiter les appels d'urgence et reconnus comme tels par un Etat membre, y compris les services de police, les services d'ambulance et les pompiers, dans le but de réagir à de tels appels.

Art. 11. Renvoi automatique d'appel

Les Etats membres veillent à ce que tout abonné ait la possibilité, par un moyen simple et gratuit, de mettre fin au renvoi automatique des appels par un tiers vers son terminal.

Art. 12. Annuaire d'abonnés

1. Les Etats membres veillent à ce que les abonnés soient informés gratuitement et avant d'y être inscrits des fins auxquelles sont établis des annuaires d'abonnés imprimés ou électroniques accessibles au public ou consultables par l'intermédiaire de services de renseignements, dans lesquels les données à caractère personnel les concernant peuvent figurer, ainsi que de toute autre possibilité d'utilisation reposant sur des fonctions de recherche intégrées dans les versions électroniques des annuaires.

2. Les Etats membres veillent à ce que les abonnés aient la possibilité de décider si les données à caractère personnel les concernant, et lesquelles de ces données, doivent figurer dans un annuaire public, dans la mesure où ces données sont pertinentes par rapport à la fonction de l'annuaire en question telle qu'elle a été établie par le fournisseur de l'annuaire. Ils font également en sorte que les abonnés puissent vérifier, corriger ou supprimer ces données. La non-inscription dans un annuaire public d'abonnés, la vérification, la correction ou la suppression de données à caractère personnel dans un tel annuaire est gratuite.

3. Les Etats membres peuvent demander que le consentement des abonnés soit également requis pour toute finalité d'annuaire public autre que la simple recherche des coordonnées d'une personne sur la base de son nom et, au besoin, d'un nombre limité d'autres paramètres.

4. Les paragraphes 1 et 2 s'appliquent aux abonnés qui sont des personnes physiques. Les Etats membres veillent également, dans le cadre du droit communautaire et des législations nationales applicables, à ce que les intérêts légitimes des abonnés autres que les personnes physiques soient suffisamment protégés en ce qui concerne leur inscription dans des annuaires publics.

Art. 13. Communications non sollicitées

1. L'utilisation de systèmes automatisés d'appel sans intervention humaine (automates d'appel), de télécopieurs ou de courrier électronique à des fins de prospection directe ne peut être autorisée que si elle vise des abonnés ayant donné leur consentement préalable.

2. Nonobstant le paragraphe 1^{er}, lorsque, dans le respect de la directive 95/46/CE, une personne physique ou morale a, dans le cadre d'une vente d'un produit ou d'un service, obtenu directement de ses clients leurs coordonnées électroniques en vue d'un courrier électronique, ladite personne physique ou morale peut exploiter ces coordonnées électroniques à des fins de prospection directe pour des produits ou services analogues qu'elle-même fournit pour autant que lesdits clients se voient donner clairement et expressément la faculté de s'opposer, sans frais et de manière simple, à une telle exploitation des coordonnées électroniques lorsqu'elles sont recueillies et lors de chaque message, au cas où ils n'auraient pas refusé d'emblée une telle exploitation.

3. Les Etats membres prennent les mesures appropriées pour que, sans frais pour l'abonné, les communications non sollicitées par celui-ci et effectuées à des fins de prospection directe, dans les cas autres que ceux visés aux paragraphes 1 et 2 ne soient pas autorisées, soit sans le consentement des abonnés concernés, soit à l'égard des abonnés qui ne souhaitent pas recevoir ces communications, le choix entre ces deux solutions étant régi par la législation nationale.

4. Dans tous les cas, il est interdit d'émettre des messages électroniques à des fins de prospection directe en camouflant ou en dissimulant l'identité de l'émetteur au nom duquel la communication est faite, ou sans indiquer d'adresse valable à laquelle le destinataire peut transmettre une demande visant à obtenir que ces communications cessent.

5. Les paragraphes 1 et 3 s'appliquent aux abonnés qui sont des personnes physiques. Les Etats membres veillent également, dans le cadre du droit communautaire et des législations nationales applicables, à ce que les intérêts légitimes des abonnés autres que les personnes physiques soient suffisamment protégés en ce qui concerne les communications non sollicitées.

Art. 14. Caractéristiques techniques et normalisation

1. Lors de la mise en oeuvre des dispositions de la présente directive, les Etats membres veillent, sous réserve des paragraphes 2 et 3, à ce qu'aucune exigence relative à des caractéristiques techniques spécifiques ne soit imposée aux terminaux ou à d'autres équipements de communications électroniques si elle risque d'entraver la mise sur le marché d'équipements et la libre circulation de ces équipements dans les Etats membres et entre ces derniers.

2. Lorsque des dispositions de la présente directive ne peuvent être mises en oeuvre qu'en imposant des caractéristiques techniques spécifiques aux réseaux de communications électroniques, les Etats membres en informent la Commission, conformément aux procédures prévues par la directive 98/34/CE du Parlement européen et du Conseil du 22 juin 1998 prévoyant une procédure d'information dans le domaine des normes et réglementations techniques et des règles relatives aux services de la société de l'information¹.

3. Au besoin, des mesures peuvent être adoptées afin de garantir que les équipements terminaux seront construits de manière compatible avec le droit des utilisateurs de protéger et de contrôler l'utilisation de leurs données à caractère personnel, conformément à la directive 1999/5/CE et à la décision 87/95/CEE du Conseil du 22 décembre 1986 relative à la normalisation dans le domaine des technologies de l'information et des télécommunications².

Art. 15. Application de certaines dispositions de la directive 95/46/CE

1. Les Etats membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale - c'est-à-dire la sûreté de l'Etat - la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1^{er}, de la directive 95/46/CE. À cette fin, les Etats membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne.

2. Les dispositions du chapitre III de la directive 95/46/CE relatif aux recours juridictionnels, à la responsabilité et aux sanctions sont applicables aux dispositions nationales adoptées en application de la présente directive ainsi qu'aux droits individuels résultant de la présente directive.

3. Le groupe de protection des personnes à l'égard du traitement des données à caractère personnel, institué par l'article 29 de la directive 95/46/CE, remplit aussi les tâches visées à l'article 30 de ladite directive en ce qui concerne les matières couvertes par la présente directive, à savoir la protection des droits et des libertés fondamentaux ainsi que des intérêts légitimes dans le secteur des communications électroniques.

Art. 16. Dispositions transitoires

1. L'article 12 ne s'applique pas aux éditions d'annuaires qui ont déjà été établies ou commercialisées en version papier ou en version électronique hors ligne avant l'entrée en vigueur des dispositions nationales adoptées en application de la présente directive.

2. Si les données à caractère personnel concernant des abonnés à des services publics de téléphonie vocale fixe ou mobile ont été insérées dans un annuaire public d'abonnés conformément aux dispositions de la directive 95/46/CE et de l'article 11 de la directive 97/66/CE avant que ne soient entrées en vigueur les dispositions de droit interne prises par les Etats membres pour se conformer à la présente directive, les données à caractère personnel desdits abonnés peuvent continuer de figurer dans cet annuaire public dans sa version papier ou électronique, y compris les versions dotées de fonctions de recherche inverse, sauf si lesdits abonnés, après avoir été pleinement informés de leurs droits et des fins auxquelles l'annuaire est établi, conformément à l'article 12 de la présente directive, s'y opposent.

Art. 17. Transposition

1. Les Etats membres mettent en vigueur avant le 31 octobre 2003 les dispositions nécessaires pour se conformer à la présente directive. Ils en informent immédiatement la Commission.

¹ JO L 204 du 21.7.1998, p. 37. Directive modifiée par la directive 98/48/CE (JO L 217 du 5.8.1998, p. 18).

² JO L 36 du 7.2.1987, p. 31. Décision modifiée en dernier lieu par l'acte d'adhésion de 1994.

Lorsque les Etats membres adoptent ces dispositions, celles-ci contiennent une référence à la présente directive ou sont accompagnées d'une telle référence lors de leur publication officielle. Les modalités de cette référence sont arrêtées par les Etats membres.

2. Les Etats membres communiquent à la Commission le texte des dispositions de droit interne qu'ils adoptent dans le domaine régi par la présente directive, ainsi que de toute modification ultérieure de ces dispositions.

Art. 18. Réexamen

Au plus tard trois ans après la date visée à l'article 17, paragraphe 1^{er}, la Commission présente au Parlement européen et au Conseil un rapport sur l'application de la présente directive et sur son impact sur les opérateurs économiques et les consommateurs, notamment en ce qui concerne les dispositions relatives aux communications non sollicitées, en prenant en considération l'environnement international. À cette fin, la Commission peut demander des informations aux Etats membres, lesquelles doivent être fournies sans retard indû. Le cas échéant, la Commission soumet des propositions de modification de la présente directive, en tenant compte des conclusions du rapport susmentionné, de tout changement intervenu dans le secteur ainsi que de toute autre proposition qu'elle peut juger nécessaire afin d'améliorer l'efficacité de la présente directive.

Art. 19. Abrogation

La directive 97/66/CE est abrogée avec effet à partir de la date visée à l'article 17, paragraphe 1^{er}.

Les références faites à la directive abrogée s'entendent comme étant faites à la présente directive.

Art. 20. Entrée en vigueur

La présente directive entre en vigueur le jour de sa publication au Journal officiel des Communautés européennes.

Art. 21. Destinataires

Les Etats membres sont destinataires de la présente directive.

Autres références.

Article 6 du Traité de l'Union européenne.
disponible depuis www.europa.eu.int

Articles 7 et 8 de la Charte des droits fondamentaux de l'Union Européenne.
disponible depuis www.europarl.eu.int

Article 8 de la Convention européenne des droits de l'homme du 4 novembre 1950.
disponible depuis <http://www.echr.coe.int>

Règlement n° 45/2001/CE du Parlement européen et du Conseil, du 18 décembre 2000, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, JOCE, L 008, 12 janv. 2001, pp. 1-22.

Décision n° 2000/519/CE de la Commission du 26 juillet 2000 relative à la constatation, conformément à la directive 95/46/CE du Parlement européen et du Conseil, du caractère adéquat de la protection des données à caractère personnel en Hongrie, JOCE, L 215, du 25 août 2000, pp. 4-6.

Décision n° 2000/518/CE de la Commission du 26 juillet 2000 relative à la constatation, conformément à la directive 95/46/CE du Parlement européen et du Conseil, du caractère adéquat de la protection des données à caractère personnel en Suisse, JOCE, L 215, du 25 août 2000, pp. 1-3.

Décision n° 2000/520/CE de la Commission du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la «sphère de sécurité» et par les questions souvent posées y afférentes, publiés par le ministère du commerce des Etats-Unis d'Amérique, JOCE, L 215, du 25 août 2000, pp. 7-47.

Décision n° 2002/2/CE de la Commission du 20 décembre 2001 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par la loi canadienne sur la protection des renseignements personnels et les documents électroniques, JOCE, L 002, du 04 janvier 2002, pp. 13-16.

Décision de la Commission du 30/06/2003 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par l'Argentine (C(2003)1731 final)

disponible depuis: http://www.europa.eu.int/comm/internal_market/privacy/docs/adequacy/decision-c2003-1731/decision-argentine_fr.pdf

III - Textes internationaux

Convention n° 108 du Conseil de l'Europe, du 28 janvier 1981, pour la protection des personnes à l'égard du traitement des données à caractère personnel.

Préambule

Les Etats membres du Conseil de l'Europe, signataires de la présente Convention,

Considérant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres, dans le respect notamment de la prééminence du droit ainsi que des droits de l'homme et des libertés fondamentales;

Considérant qu'il est souhaitable d'étendre la protection des droits et des libertés fondamentales de chacun, notamment le droit au respect de la vie privée, eu égard à l'intensification de la circulation à travers les frontières des données à caractère personnel faisant l'objet de traitements automatisés;

Réaffirmant en même temps leur engagement en faveur de la liberté d'information sans considération de frontières;

Reconnaissant la nécessité de concilier les valeurs fondamentales du respect de la vie privée et de la libre circulation de l'information entre les peuples,

Sont convenus de ce qui suit:

Chapitre I^{er}. – Dispositions générales

Art. 1^{er}. – Objet et but

Le but de la présente Convention est de garantir, sur le territoire de chaque Partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant («protection des données»).

Art. 2. – Définitions

Aux fins de la présente Convention:

«données à caractère personnel» signifie: toute information concernant une personne physique identifiée ou identifiable («personne concernée»);

«fichier automatisé» signifie: tout ensemble d'informations faisant l'objet d'un traitement automatisé;

«traitement automatisé» s'entend des opérations suivantes effectuées en totalité ou en partie à l'aide de procédés automatisés: enregistrement des données, application à ces données d'opérations logiques et/ou arithmétiques, leur modification, effacement, extraction ou diffusion;

«maître du fichier» signifie: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui est compétent selon la loi nationale, pour décider quelle sera la finalité du fichier automatisé, quelles catégories de données à caractère personnel doivent être enregistrées et quelles opérations leur seront appliquées.

Art. 3. – Champ d'application

Les Parties s'engagent à appliquer la présente Convention aux fichiers et aux traitements automatisés de données à caractère personnel dans les secteurs public et privé.

Tout Etat peut, lors de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, ou à tout moment ultérieur, faire connaître par déclaration adressée au Secrétaire Général du Conseil de l'Europe:

qu'il n'appliquera pas la présente Convention à certaines catégories de fichiers automatisés de données à caractère personnel dont une liste sera déposée. Il ne devra toutefois pas inclure dans cette liste des catégories de fichiers automatisés assujetties selon son droit interne à des dispositions de protection des données. En conséquence, il devra amender cette liste par une nouvelle déclaration

lorsque des catégories supplémentaires de fichiers automatisés de données à caractère personnel seront assujetties à son régime de protection des données;

qu'il appliquera la présente Convention également à des informations afférentes à des groupements, associations, fondations, sociétés, corporations ou à tout autre organisme regroupant directement ou indirectement des personnes physiques et jouissant ou non de la personnalité juridique;

qu'il appliquera la présente Convention également aux fichiers de données à caractère personnel ne faisant pas l'objet de traitements automatisés.

Tout Etat qui a étendu le champ d'application de la présente Convention par l'une des déclarations visées aux alinéas 2.b ou c ci-dessus peut, dans ladite déclaration, indiquer que les extensions ne s'appliqueront qu'à certaines catégories de fichiers à caractère personnel dont la liste sera déposée.

Toute Partie qui a exclu certaines catégories de fichiers automatisés de données à caractère personnel par la déclaration prévue à l'alinéa 2.a ci-dessus ne peut pas prétendre à l'application de la présente Convention à de telles catégories par une Partie qui ne les a pas exclues.

De même, une Partie qui n'a pas procédé à l'une ou à l'autre des extensions prévues aux paragraphes 2.b et c du présent article ne peut se prévaloir de l'application de la présente Convention sur ces points à l'égard d'une Partie qui a procédé à de telles extensions.

Les déclarations prévues au paragraphe 2 du présent article prendront effet au moment de l'entrée en vigueur de la Convention à l'égard de l'Etat qui les a formulées, si cet Etat les a faites lors de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, ou trois mois après leur réception par le Secrétaire Général du Conseil de l'Europe si elles ont été formulées à un moment ultérieur. Ces déclarations pourront être retirées en tout ou en partie par notification adressée au Secrétaire Général du Conseil de l'Europe. Le retrait prendra effet trois mois après la date de réception d'une telle notification.

Chapitre II. – Principes de base pour la protection des données

Art. 4. – Engagements des Parties

Chaque Partie prend, dans son droit interne, les mesures nécessaires pour donner effet aux principes de base pour la protection des données énoncés dans le présent chapitre.

Ces mesures doivent être prises au plus tard au moment de l'entrée en vigueur de la présente Convention à son égard.

Art. 5. – Qualité des données

Les données à caractère personnel faisant l'objet d'un traitement automatisé sont:

obtenues et traitées loyalement et licitement;

enregistrées pour des finalités déterminées et légitimes et ne sont pas utilisées de manière incompatible avec ces finalités;

adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées;

exactes et si nécessaire mises à jour;

conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées.

Art. 6. – Catégories particulières de données

Les données à caractère personnel 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, ne peuvent être traitées automatiquement à moins que le droit interne ne prévoie des garanties appropriées. Il en est de même des données à caractère personnel concernant des condamnations pénales.

Art. 7. – Sécurité des données

Des mesures de sécurité appropriées sont prises pour la protection des données à caractère personnel enregistrées dans des fichiers automatisés contre la destruction accidentelle ou non autorisée, ou la perte accidentelle, ainsi que contre l'accès, la modification ou la diffusion non autorisés.

Art. 8. – Garanties complémentaires pour la personne concernée

Toute personne doit pouvoir:

connaître 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; obtenir à des intervalles raisonnables et sans délais ou frais excessifs la confirmation de l'existence ou non dans le fichier automatisé, de données à caractère personnel la concernant ainsi que la communication de ces données sous une forme intelligible;

obtenir, le cas échéant, la rectification de ces données ou leur effacement lorsqu'elles ont été traitées en violation des dispositions du droit interne donnant effet aux principes de base énoncés dans les articles 5 et 6 de la présente Convention;

disposer d'un recours s'il n'est pas donné suite à une demande de confirmation ou, le cas échéant, de communication, de rectification ou d'effacement, visée aux paragraphes b et c du présent article.

Art. 9. – Exceptions et restrictions

Aucune exception aux dispositions des articles 5, 6 et 8 de la présente Convention n'est admise, sauf dans les limites définies au présent article.

Il est possible de déroger aux dispositions des articles 5, 6 et 8 de la présente Convention lorsqu'une telle dérogation, prévue par la loi de la Partie, constitue une mesure nécessaire dans une société démocratique:

à la protection de la sécurité de l'Etat, à la sûreté publique, aux intérêts monétaires de l'Etat ou à la répression des infractions pénales;

à la protection de la personne concernée et des droits et libertés d'autrui.

Des restrictions à l'exercice des droits visés aux paragraphes b, c et d de l'article 8 peuvent être prévues par la loi pour les fichiers automatisés de données à caractère personnel utilisés à des fins de statistiques ou de recherches scientifiques, lorsqu'il n'existe manifestement pas de risques d'atteinte à la vie privée des personnes concernées.

Art. 10. – Sanctions et recours

Chaque Partie s'engage à établir des sanctions et recours appropriés visant les violations aux dispositions du droit interne donnant effet aux principes de base pour la protection des données énoncés dans le présent chapitre.

Art. 11. – Protection plus étendue

Aucune des dispositions du présent chapitre ne sera interprétée comme limitant ou portant atteinte à la faculté pour chaque Partie d'accorder aux personnes concernées une protection plus étendue que celle prévue par la présente Convention.

Chapitre III. – Flux transfrontières de données**Art. 12. – Flux transfrontières de données à caractère personnel et droit interne**

Les dispositions suivantes s'appliquent aux transferts à travers les frontières nationales, quel que soit le support utilisé, de données à caractère personnel faisant l'objet d'un traitement automatisé ou rassemblées dans le but de les soumettre à un tel traitement.

Une Partie ne peut pas, aux seules fins de la protection de la vie privée, interdire ou soumettre à une autorisation spéciale les flux transfrontières de données à caractère personnel à destination du territoire d'une autre Partie.

Toutefois, toute Partie a la faculté de déroger aux dispositions du paragraphe 2:

dans la mesure où sa législation prévoit une réglementation spécifique pour certaines catégories de données à caractère personnel ou de fichiers automatisés de données à caractère personnel, en raison de la nature de ces données ou de ces fichiers, sauf si la réglementation de l'autre Partie apporte une protection équivalente;

lorsque le transfert est effectué à partir de son territoire vers le territoire d'un Etat non contractant par l'intermédiaire du territoire d'une autre Partie, afin d'éviter que de tels transferts n'aboutissent à contourner la législation de la Partie visée au début du présent paragraphe.

Chapitre IV. – Entraide

Art. 13. – Coopération entre les Parties

Les Parties s'engagent à s'accorder mutuellement assistance pour la mise en œuvre de la présente Convention.

A cette fin,

chaque Partie désigne une ou plusieurs autorités dont elle communique la dénomination et l'adresse au Secrétaire Général du Conseil de l'Europe;

chaque Partie qui a désigné plusieurs autorités indique dans la communication visée à l'alinéa précédent la compétence de chacune de ces autorités.

Une autorité désignée par une Partie, à la demande d'une autorité désignée par une autre Partie:

fournira des informations sur son droit et sur sa pratique administrative en matière de protection des données;

prendra, conformément à son droit interne et aux seules fins de la protection de la vie privée, toutes mesures appropriées pour fournir des informations de fait concernant un traitement automatisé déterminé effectué sur son territoire à l'exception toutefois des données à caractère personnel faisant l'objet de ce traitement.

Art. 14. – Assistance aux personnes concernées ayant leur résidence à l'étranger

Chaque Partie prête assistance à toute personne ayant sa résidence à l'étranger pour l'exercice des droits prévus par son droit interne donnant effet aux principes énoncés à l'article 8 de la présente Convention.

Si une telle personne réside sur le territoire d'une autre Partie, elle doit avoir la faculté de présenter sa demande par l'intermédiaire de l'autorité désignée par cette Partie.

La demande d'assistance doit contenir toutes les indications nécessaires concernant notamment:

le nom, l'adresse et tous autres éléments pertinents d'identification concernant le requérant;

le fichier automatisé de données à caractère personnel auquel la demande se réfère ou le maître de ce fichier;

le but de la demande.

Art. 15. – Garanties concernant l'assistance fournie par les autorités désignées

Une autorité désignée par une Partie qui a reçu des informations d'une autorité désignée par une autre Partie, soit à l'appui d'une demande d'assistance, soit en réponse à une demande d'assistance qu'elle a formulée elle-même, ne pourra faire usage de ces informations à des fins autres que celles spécifiées dans la demande d'assistance.

Chaque Partie veillera à ce que les personnes appartenant ou agissant au nom de l'autorité désignée soient liées par des obligations appropriées de secret ou de confidentialité à l'égard de ces informations.

En aucun cas, une autorité désignée ne sera autorisée à faire, aux termes de l'article 14, paragraphe 2, une demande d'assistance au nom d'une personne concernée résidant à l'étranger, de sa propre initiative et sans le consentement exprès de cette personne.

Art. 16. – Refus des demandes d'assistance

Une autorité désignée, saisie d'une demande d'assistance aux termes des articles 13 ou 14 de la présente Convention, ne peut refuser d'y donner suite que si:

la demande est incompatible avec les compétences, dans le domaine de la protection des données, des autorités habilitées à répondre;

la demande n'est pas conforme aux dispositions de la présente Convention;

l'exécution de la demande serait incompatible avec la souveraineté, la sécurité ou l'ordre public de la Partie qui l'a désignée, ou avec les droits et libertés fondamentales des personnes relevant de la juridiction de cette Partie.

Art. 17 – Frais et procédures de l'assistance

L'entraide que les Parties s'accordent aux termes de l'article 13, ainsi que l'assistance qu'elles prêtent aux personnes concernées résidant à l'étranger aux termes de l'article 14, ne donnera pas lieu au paiement

des frais et droits autres que ceux afférents aux experts et aux interprètes. Ces frais et droits seront à la charge de la Partie qui a désigné l'autorité qui a fait la demande d'assistance.

La personne concernée ne peut être tenue de payer, en liaison avec les démarches entreprises pour son compte sur le territoire d'une autre Partie, des frais et droits autres que ceux exigibles des personnes résidant sur le territoire de cette Partie.

Les autres modalités relatives à l'assistance concernant notamment les formes et procédures ainsi que les langues à utiliser seront établies directement entre les Parties concernées.

Chapitre V. – Comité consultatif

Art. 18 – Composition du comité

Un comité consultatif est constitué après l'entrée en vigueur de la présente Convention.

Toute Partie désigne un représentant et un suppléant à ce comité. Tout Etat membre du Conseil de l'Europe qui n'est pas Partie à la Convention a le droit de se faire représenter au comité par un observateur.

Le comité consultatif peut, par une décision prise à l'unanimité, inviter tout Etat non membre du Conseil de l'Europe qui n'est pas Partie à la Convention à se faire représenter par un observateur à l'une de ses réunions.

Art. 19. – Fonctions du comité

Le comité consultatif:

- peut faire des propositions en vue de faciliter ou d'améliorer l'application de la Convention;
- peut faire des propositions d'amendement à la présente Convention conformément à l'article 21;
- formule un avis sur toute proposition d'amendement à la présente Convention qui lui est soumis conformément à l'article 21 , paragraphe 3;
- peut, à la demande d'une Partie, exprimer un avis sur toute question relative à l'application de la présente Convention.

Art. 20. – Procédure

Le comité consultatif est convoqué par le Secrétaire Général du Conseil de l'Europe. Il tient sa première réunion dans les douze mois qui suivent l'entrée en vigueur de la présente Convention. Il se réunit par la suite au moins une fois tous les deux ans et, en tout cas, chaque fois qu'un tiers des représentants des Parties demande sa convocation.

La majorité des représentants des Parties constitue le quorum nécessaire pour tenir une réunion du comité consultatif.

A l'issue de chacune de ses réunions, le comité consultatif soumet au Comité des Ministres du Conseil de l'Europe un rapport sur ses travaux et sur le fonctionnement de la Convention.

Sous réserve des dispositions de la présente Convention, le Comité consultatif établit son règlement intérieur.

Chapitre VI. – Amendements

Art. 21. – Amendements

Des amendements à la présente Convention peuvent être proposés par une Partie, par le Comité des Ministres du Conseil de l'Europe ou par le comité consultatif.

Toute proposition d'amendement est communiquée par le Secrétaire Général du Conseil de l'Europe aux Etats membres du Conseil de l'Europe et à chaque Etat non membre qui a adhéré ou a été invité à adhérer à la présente Convention conformément aux dispositions de l'article 23.

En outre, tout amendement proposé par une Partie ou par le Comité des Ministres est communiqué au comité consultatif qui soumet au Comité des Ministres son avis sur l'amendement proposé.

Le Comité des Ministres examine l'amendement proposé et tout avis soumis par le comité consultatif et peut approuver l'amendement.

Le texte de tout amendement approuvé par le Comité des Ministres conformément au paragraphe 4 du présent article est transmis aux Parties pour acceptation.

Tout amendement approuvé conformément au paragraphe 4 du présent article entrera en vigueur le trentième jour après que toutes les Parties auront informé le Secrétaire Général qu'elles l'ont accepté.

Chapitre VII. – Clauses finales

Art. 22. – Entrée en vigueur

La présente Convention est ouverte à la signature des Etats membres du Conseil de l'Europe. Elle sera soumise à ratification, acceptation ou approbation. Les instruments de ratification, d'acceptation ou d'approbation seront déposés près le Secrétaire Général du Conseil de l'Europe.

La présente Convention entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date à laquelle cinq Etats membres du Conseil de l'Europe auront exprimé leur consentement à être liés par la Convention conformément aux dispositions du paragraphe précédent.

Pour tout Etat membre qui exprimera ultérieurement son consentement à être lié par la Convention, celle-ci entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date du dépôt de l'instrument de ratification, d'acceptation ou d'approbation.

Art. 23. – Adhésion d'Etats non membres

Après l'entrée en vigueur de la présente Convention, le Comité des Ministres du Conseil de l'Europe pourra inviter tout Etat non membre du Conseil de l'Europe à adhérer à la présente Convention par une décision prise à la majorité prévue à l'article 20.d du Statut du Conseil de l'Europe et à l'unanimité des représentants des Etats contractants ayant le droit de siéger au comité.

Pour tout Etat adhérent, la Convention entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date du dépôt de l'instrument d'adhésion près le Secrétaire Général du Conseil de l'Europe.

Art. 24. – Clause territoriale

Tout Etat peut, au moment de la signature ou au moment du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, désigner le ou les territoires auxquels s'appliquera la présente Convention.

Tout Etat peut, à tout autre moment par la suite, par une déclaration adressée au Secrétaire Général du Conseil de l'Europe, étendre l'application de la présente Convention à tout autre territoire désigné dans la déclaration. La Convention entrera en vigueur à l'égard de ce territoire le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de la déclaration par le Secrétaire Général.

Toute déclaration faite en vertu des deux paragraphes précédents pourra être retirée, en ce qui concerne tout territoire désigné dans cette déclaration, par notification adressée au Secrétaire Général. Le retrait prendra effet le premier jour du mois qui suit l'expiration d'une période de six mois après la date de réception de la notification par le Secrétaire Général.

Art. 25. – Réserves

Aucune réserve n'est admise aux dispositions de la présente Convention.

Art. 26. – Dénonciation

Toute Partie peut, à tout moment, dénoncer la présente Convention en adressant une notification au Secrétaire Général du Conseil de l'Europe.

La dénonciation prendra effet le premier jour du mois qui suit l'expiration d'une période de six mois après la date de réception de la notification par le Secrétaire Général.

Art. 27. – Notifications

Le Secrétaire Général du Conseil de l'Europe notifiera aux Etats membres du Conseil et à tout Etat ayant adhéré à la présente Convention:

toute signature;

le dépôt de tout instrument de ratification, d'acceptation, d'approbation ou d'adhésion;

toute date d'entrée en vigueur de la présente Convention conformément à ses articles 22, 23 et 24;

tout autre acte, notification ou communication ayant trait à la présente Convention.

Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, du 8 novembre 2001 concernant les autorités de contrôle et les flux transfrontières de données.

Préambule

Les Parties au présent Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, ouverte à la signature à Strasbourg, le 28 janvier 1981, (ci-après dénommé «la Convention»),

Convaincues que des autorités de contrôle exerçant leurs fonctions en toute indépendance sont un élément de la protection effective des personnes à l'égard du traitement des données à caractère personnel;

Considérant l'importance de la circulation de l'information entre les peuples;

Considérant que, avec l'intensification des échanges de données à caractère personnel à travers les frontières, il est nécessaire d'assurer la protection effective des droits de l'homme et des libertés fondamentales, et, notamment du droit au respect de la vie privée, en relation avec de tels échanges,

Sont convenues de ce qui suit:

Art. 1^{er}. – Autorités de contrôle

1. Chaque Partie prévoit qu'une ou plusieurs autorités sont chargées de veiller au respect des mesures donnant effet, dans son droit interne, aux principes énoncés dans les chapitres II et III de la Convention et dans le présent Protocole.

2. a. A cet effet, ces autorités disposent notamment de pouvoirs d'investigation et d'intervention, ainsi que de celui d'ester en justice ou de porter à la connaissance de l'autorité judiciaire compétente des violations aux dispositions du droit interne donnant effet aux principes visés au paragraphe 1 de l'article 1 du présent Protocole.

b. Chaque autorité de contrôle peut être saisie par toute personne d'une demande relative à la protection de ses droits et libertés fondamentales à l'égard des traitements de données à caractère personnel relevant de sa compétence.

3. Les autorités de contrôle exercent leurs fonctions en toute indépendance.

4. Les décisions des autorités de contrôle faisant grief peuvent faire l'objet d'un recours juridictionnel.

5. Conformément aux dispositions du chapitre IV et sans préjudice des dispositions de l'article 13 de la Convention, les autorités de contrôle coopèrent entre elles dans la mesure nécessaire à l'accomplissement de leurs missions, notamment en échangeant toute information utile.

Art. 2. – Flux transfrontières de données à caractère personnel vers un destinataire n'étant pas soumis à la juridiction d'une Partie à la Convention

1. Chaque Partie prévoit que le transfert de données à caractère personnel vers un destinataire soumis à la juridiction d'un Etat ou d'une organisation qui n'est pas Partie à la Convention ne peut être effectué que si cet Etat ou cette organisation assure un niveau de protection adéquat pour le transfert considéré.

2. Par dérogation au paragraphe 1^{er} de l'article 2 du présent Protocole, chaque Partie peut autoriser un transfert de données à caractère personnel:

a. si le droit interne le prévoit:

- pour des intérêts spécifiques de la personne concernée, ou
- lorsque des intérêts légitimes prévalent, en particulier des intérêts publics importants, ou

b. si des garanties pouvant notamment résulter de clauses contractuelles sont fournies par la personne responsable du transfert, et sont jugées suffisantes par les autorités compétentes, conformément au droit interne.

Art. 3. – Dispositions finales

1. Les Parties considèrent les dispositions des articles 1 et 2 du présent Protocole comme des articles additionnels à la Convention, et toutes les dispositions de la Convention s'appliquent en conséquence.

2. Le présent Protocole est ouvert à la signature des Etats signataires de la Convention. Après avoir adhéré à la Convention dans les conditions établies par celle-ci, les Communautés européennes peuvent signer le présent Protocole. Ce Protocole sera soumis à ratification, acceptation ou approbation. Un Signataire du présent Protocole ne peut le ratifier, l'accepter ou l'approuver, sans avoir antérieurement ou simultanément ratifié, accepté ou approuvé la Convention ou sans y avoir adhéré. Les instruments de ratification, d'acceptation ou d'approbation du présent Protocole seront déposés près le Secrétaire Général du Conseil de l'Europe.

3. a. Le présent Protocole entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date à laquelle cinq de ses Signataires auront exprimé leur consentement à être liés par le présent Protocole conformément aux dispositions de son article 3 paragraphe 2.

b. Pour tout Signataire du présent Protocole qui exprime ultérieurement son consentement à être lié par celui-ci, le présent Protocole entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date du dépôt de son instrument de ratification, d'acceptation ou d'approbation.

4. a. Après l'entrée en vigueur du présent Protocole, tout Etat qui a adhéré à la Convention pourra adhérer également au présent Protocole.

b. L'adhésion s'effectuera par le dépôt, près le Secrétaire Général du Conseil de l'Europe, d'un instrument d'adhésion qui prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de son dépôt.

5. a. Toute Partie peut, à tout moment, dénoncer le présent Protocole en adressant une notification au Secrétaire Général du Conseil de l'Europe.

b. La dénonciation prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de la notification par le Secrétaire Général.

6. Le Secrétaire Général du Conseil de l'Europe notifiera aux Etats membres du Conseil de l'Europe, aux Communautés européennes et à tout Etat ayant adhéré au présent Protocole:

a. toute signature;

b. le dépôt de tout instrument de ratification, d'acceptation ou d'approbation;

c. toute date d'entrée en vigueur du présent Protocole conformément à son article 3;

d. tout autre acte, notification ou communication ayant trait au présent Protocole.

Autres références.

Les «Principes directeurs pour la réglementation des fichiers personnels informatisés» adoptés par l'Assemblée Générale des nations unies le 14 décembre 1990

disponible depuis <http://www.un.org>

La recommandation de l'OCDE, du 23 septembre 1980, concernant la vie privée et les flux transfrontaliers de données personnelles, la déclaration des Ministres de l'OCDE du 11 avril 1985 sur les flux transfrontaliers de données personnelles et la déclaration des Ministres de l'OCDE du 7-9 octobre 1998 sur la vie privée dans les réseaux mondiaux

disponible depuis <http://www.oecd.org>

Recommandation N° R (2002) 9 du Conseil des Ministres du Conseil de l'Europe, du 18 septembre 2002, sur la protection des données à caractère personnel collectées et traitées à des fins d'assurance, et Exposé des motifs

disponible depuis <http://www.coe.int>

Recommandation N° R (99) 5 du Conseil des Ministres du Conseil de l'Europe, du 23 février 1999, sur la protection de la vie privée sur Internet

disponible depuis <http://www.coe.int>

Recommandation N° R (97) 18 du Conseil des Ministres du Conseil de l'Europe, du 30 septembre 1997, sur la protection des données à caractère personnel collectées et traitées à des fins statistiques et Exposé des motifs

disponible depuis <http://www.coe.int>

Recommandation N° R (97) 5 du Conseil des Ministres du Conseil de l'Europe, du 13 février 1997, sur la protection des données médicales et Exposé des motifs

disponible depuis <http://www.coe.int>

Recommandation N° R (95) 4 du Conseil des Ministres du Conseil de l'Europe, du 7 février 1995, sur la protection des données à caractère personnel dans le domaine des services de télécommunications, eu égard notamment aux services téléphoniques et Exposé des motifs

disponible depuis <http://www.coe.int>

Recommandation N° R (91) 10 du Conseil des Ministres du Conseil de l'Europe, du 9 septembre 1991, sur la communication à des tierces personnes de données à caractère personnel détenues par des organismes publics et Exposé des motifs

disponible depuis <http://www.coe.int>

Recommandation N° R (90) 19 du Conseil des Ministres du Conseil de l'Europe, du 13 septembre 1990, sur la protection des données à caractère personnel utilisées à des fins de paiement et autres opérations connexes et Exposé des motifs

disponible depuis <http://www.coe.int>

Recommandation N° R (89) 2 du Conseil des Ministres du Conseil de l'Europe, du 18 janvier 1989, sur la protection des données à caractère personnel utilisées à des fins d'emploi et Exposé des motifs

disponible depuis <http://www.coe.int>

Recommandation N° R (87) 15 du Conseil des Ministres du Conseil de l'Europe, du 17 septembre 1987, visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police et les rapports d'évaluation de la Recommandation : Premier (1994), Deuxième (1998) et Troisième (2002)

disponible depuis <http://www.coe.int>

Recommandation N° R (86) 1 du Conseil des Ministres du Conseil de l'Europe, du 23 janvier 1986, relative à la protection des données à caractère personnel utilisées à des fins de sécurité sociale et Exposé des motifs

disponible depuis <http://www.coe.int>

Recommandation N° R (85) 20 du Conseil des Ministres du Conseil de l'Europe, du 25 octobre 1985, relative à la protection des données à caractère personnel utilisées à des fins de marketing direct

disponible depuis <http://www.coe.int>

Résolution (74) 29 du Conseil des Ministres du Conseil de l'Europe sur la protection des données à caractère personnel dans les traitements automatiques de banques de données dans les secteurs public

disponible depuis <http://www.coe.int>

Résolution (73) 22 du Conseil des Ministres du Conseil de l'Europe sur la protection des données à caractère personnel dans les traitements automatiques de banques de données dans les secteurs privé

disponible depuis <http://www.coe.int>
