►**B** **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 (directive vie privée et communications électroniques)

(JO L 201 du 31.7.2002, p. 37)

Modifiée par:

		Journal officiel		
		n°	page	date
►**M1**	Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006	L 105	54	13.4.2006
►**M2**	Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009	L 337	11	18.12.2009

Rectifié par:

►**C1** Rectificatif, JO L 241 du 10.9.2013, p. 9 (2009/136/CE)

▼B

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 (directive vie privée et communications électroniques)

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 Commission ([1]),

vu l'avis du Comité économique et social ([2]),

après consultation du Comité des régions,

statuant conformément à la procédure visée à l'article 251 du traité ([3]),

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 données ([4]) exige que les États 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 États membres.

([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.

▼B

(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 télécommunications ([1]) 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.

(8) Il convient d'harmoniser les dispositions législatives, réglementaires et techniques adoptées par les États 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 États membres ne sont pas entravés.

([1]) JO L 24 du 30.1.1998, p. 1.

▼B

(9) Les États 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 œuvre 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 États 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'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) et de l'application du droit pénal. Par conséquent, la présente directive ne porte pas atteinte à la faculté des États 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 États 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.

▼B

(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 États membres devraient donc les communiquer à la Commission.

▼B

(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 États 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.

▼B

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

▼B

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.

▼B

(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 États 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 États 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

▼B

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 États 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 États 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.

▼B

(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 États 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.

▼B

(43) Afin de faciliter la mise en œuvre 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 États 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 États 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 conformité ([2]) 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 œuvre du marché intérieur.

([1]) JO L 178 du 17.7.2000, p. 1.
([2]) JO L 91 du 7.4.1999, p. 10.

▼B

(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 État 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 États membres,

ONT ARRÊTÉ LA PRÉSENTE DIRECTIVE:

Article premier

Champ d'application et objectif

▼M2

1. La présente directive prévoit l'harmonisation des dispositions nationales nécessaires pour assurer un niveau équivalent de protection des droits et libertés fondamentaux, et en particulier du droit à la vie privée et à la confidentialité, 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 services de communications électroniques dans la Communauté.

▼B

2. Les dispositions de la présente directive précisent et complètent la directive 95/46/CE aux fins énoncées au paragraphe 1. En outre, elles prévoient la protection des intérêts légitimes des abonnés qui sont des personnes morales.

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'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) ou aux activités de l'État dans des domaines relevant du droit pénal.

▼B

Article 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;

▼M2

c) «données de localisation»: toutes les données traitées dans un réseau de communications électroniques ou par un service de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public;

▼B

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;

▼M2

_____

▼B

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;

([1]) JO L 108 du 24.4.2002, p. 33.

▼M2

►C1 i) «violation de données à caractère personnel»: ◄ une violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés de données à caractère personnel transmises, stockées ou traitées d'une autre manière en relation avec la fourniture de services de communications électroniques accessibles au public dans la Communauté.

Article 3

Services concernés

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 de communications publics dans la Communauté, y compris les réseaux de communications publics qui prennent en charge les dispositifs de collecte de données et d'identification.

▼B

Article 4

►M2 Sécurité du traitement ◄

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 œuvre, ces mesures garantissent un degré de sécurité adapté au risque existant.

▼M2

1 *bis*. Sans préjudice des dispositions de la directive 95/46/CE, les mesures visées au paragraphe 1, pour le moins:

— garantissent que seules des personnes autorisées peuvent avoir accès aux données à caractère personnel à des fins légalement autorisées,

— protègent les données à caractère personnel stockées ou transmises contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelles et le stockage, le traitement, l'accès et la divulgation non autorisés ou illicites, et

— assurent la mise en œuvre d'une politique de sécurité relative au traitement des données à caractère personnel.

Les autorités nationales compétentes en la matière sont habilitées à vérifier les mesures prises par les fournisseurs de services de communications électroniques accessibles au public, ainsi qu'à émettre des recommandations sur les meilleures pratiques concernant le degré de sécurité que ces mesures devraient atteindre.

▼B

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.

▼M2

3. En cas de violation de données à caractère personnel, le fournisseur de services de communications électroniques accessibles au public avertit sans retard indu l'autorité nationale compétente de la violation.

Lorsque la violation de données à caractère personnel est de nature à affecter négativement les données à caractère personnel ou la vie privée d'un abonné ou d'un particulier, le fournisseur avertit également sans retard indu l'abonné ou le particulier concerné de la violation.

La notification d'une violation des données à caractère personnel à l'abonné ou au particulier concerné n'est pas nécessaire si le fournisseur a prouvé, à la satisfaction de l'autorité compétente, qu'il a mis en œuvre les mesures de protection technologiques appropriées et que ces dernières ont été appliquées aux données concernées par ladite violation. De telles mesures de protection technologiques rendent les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès.

Sans préjudice de l'obligation du fournisseur d'informer les abonnés et les particuliers concernés, si le fournisseur n'a pas déjà averti l'abonné ou le particulier de la violation de données à caractère personnel, l'autorité nationale compétente peut, après avoir examiné les effets éventuellement négatifs de cette violation, exiger du fournisseur qu'il s'exécute.

La notification faite à l'abonné ou au particulier décrit au minimum la nature de la violation de données à caractère personnel et les points de contact auprès desquels des informations supplémentaires peuvent être obtenues et recommande des mesures à prendre pour atténuer les conséquences négatives possibles de la violation de données à caractère personnel. La notification faite à l'autorité nationale compétente décrit en outre les conséquences de la violation de données à caractère personnel, et les mesures proposées ou prises par le fournisseur pour y remédier.

4. Sous réserve des mesures techniques d'application adoptées en vertu du paragraphe 5, les autorités nationales compétentes peuvent adopter des lignes directrices et, le cas échéant, édicter des instructions précisant les circonstances dans lesquelles le fournisseur est tenu de notifier la violation de données à caractère personnel, le format applicable à cette notification et sa procédure de transmission. Elles doivent également être en mesure de contrôler si les fournisseurs ont satisfait aux obligations de notification qui leur incombent en vertu du présent paragraphe et infligent des sanctions appropriées si ces derniers ne s'y sont pas conformés.

▼M2

Les fournisseurs tiennent à jour un inventaire des violations de données à caractère personnel, notamment de leur contexte, de leurs effets et des mesures prises pour y remédier, les données consignées devant être suffisantes pour permettre aux autorités nationales compétentes de vérifier le respect des dispositions du paragraphe 3. Cet inventaire comporte uniquement les informations nécessaires à cette fin.

5. Afin d'assurer une mise en œuvre cohérente des mesures visées aux paragraphes 2, 3 et 4, la Commission peut, après consultation de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), du 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 et du Contrôleur européen de la protection des données, adopter des mesures techniques d'application concernant les circonstances, le format et les procédures applicables aux exigences en matière d'information et de notification visées au présent article. Lors de l'adoption de ces mesures, la Commission associe toutes les parties prenantes concernées, notamment pour être informée des meilleures solutions techniques et économiques disponibles pour assurer la mise en œuvre du présent article.

Ces mesures, qui visent à modifier des éléments non essentiels de la présente directive en la complétant, sont arrêtées en conformité avec la procédure de réglementation avec contrôle visée à l'article 14 *bis*, paragraphe 2.

▼B

Article 5

Confidentialité des communications

1. Les États 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 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.

▼M2

3. Les États membres garantissent que le stockage d'informations, ou l'obtention de l'accès à des informations déjà stockées, dans l'équipement terminal d'un abonné ou d'un utilisateur n'est permis qu'à condition que l'abonné ou l'utilisateur ait donné son accord, après avoir reçu, dans le respect de la directive 95/46/CE, une information claire et complète, entre autres sur les finalités du traitement. Cette disposition ne fait pas obstacle à un stockage ou à un accès techniques visant exclusivement à effectuer la transmission d'une communication par la voie d'un réseau de communications électroniques, ou strictement nécessaires au fournisseur pour la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur.

▼B

Article 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.

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.

▼M2

3. Afin de commercialiser des 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 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 préalable. Les utilisateurs ou abonnés ont la possibilité de retirer à tout moment leur consentement pour le traitement des données relatives au trafic.

▼B

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.

▼B

Article 7

Facturation détaillée

1. Les abonnés ont le droit de recevoir des factures non détaillées.

2. Les États 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.

Article 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 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 États 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.

▼B

Article 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.

Article 10

Dérogations

Les États 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

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 État membre, y compris les services de police, les services d'ambulance et les pompiers, dans le but de réagir à de tels appels.

Article 11

Renvoi automatique d'appel

Les États 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.

Article 12

Annuaires d'abonnés

1. Les États 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 États 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 États 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 États 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.

▼M2

Article 13

Communications non sollicitées

1. L'utilisation de systèmes automatisés d'appel et de communication 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 ou des utilisateurs ayant donné leur consentement préalable.

2. Nonobstant le paragraphe 1, lorsque, dans le respect de la directive 95/46/CE, une personne physique ou morale a, dans le cadre de la vente d'un produit ou d'un service, obtenu 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 au moment où elles sont recueillies et lors de chaque message, au cas où ils n'auraient pas refusé d'emblée une telle exploitation.

3. Les États membres prennent les mesures appropriées pour assurer que les communications non sollicitées 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 ou des utilisateurs concernés, soit à l'égard des abonnés ou des utilisateurs qui ne souhaitent pas recevoir ces communications, le choix entre ces deux solutions étant régi par la législation nationale, sachant que les deux solutions doivent être gratuites pour l'abonné ou l'utilisateur.

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, en violation de l'article 6 de la directive 2000/31/CE, sans indiquer d'adresse valable à laquelle le destinataire peut transmettre une demande visant à obtenir que ces communications cessent, ou en encourageant les destinataires à visiter des sites internet enfreignant ledit article.

5. Les paragraphes 1 et 3 s'appliquent aux abonnés qui sont des personnes physiques. Les États 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.

6. Sans préjudice d'éventuels recours administratifs qui peuvent être prévus notamment en vertu de l'article 15 *bis*, paragraphe 2, les États membres veillent à ce que toute personne physique ou morale ayant pâti d'infractions aux dispositions nationales adoptées en application du présent article et ayant dès lors un intérêt légitime à voir cesser ou interdire ces infractions, y compris un fournisseur de services de

▼M2

communications électroniques protégeant ses intérêts professionnels légitimes, puisse engager des actions en justice en ce qui concerne de telles infractions. Les États membres peuvent également déterminer le régime spécifique des sanctions applicables aux fournisseurs de services de communications électroniques qui, par leur négligence, contribuent aux violations des dispositions nationales prises en application du présent article.

▼B

Article 14

Caractéristiques techniques et normalisation

1. Lors de la mise en œuvre des dispositions de la présente directive, les États 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 États membres et entre ces derniers.

2. Lorsque des dispositions de la présente directive ne peuvent être mises en œuvre qu'en imposant des caractéristiques techniques spécifiques aux réseaux de communications électroniques, les États 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'information ([1]).

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 télécommunications ([2]).

▼M2

Article 14 bis

Procédure de comité

1. La Commission est assistée par le comité des communications institué par l'article 22 de la directive 2002/21/CE (directive «cadre»).

2. Dans le cas où il est fait référence au présent paragraphe, l'article 5 *bis*, paragraphes 1 à 4, et l'article 7 de la décision 1999/468/CE s'appliquent, dans le respect des dispositions de l'article 8 de celle-ci.

3. Dans le cas où il est fait référence au présent paragraphe, l'article 5 *bis*, paragraphes 1, 2, 4 et 6, et l'article 7 de la décision 1999/468/CE s'appliquent, dans le respect des dispositions de l'article 8 de celle-ci.

([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.

▼B

Article 15

Application de certaines dispositions de la directive 95/46/CE

1. Les États 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'État — 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, de la directive 95/46/CE. À cette fin, les États 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.

▼M1

1 *bis*. Le paragraphe 1 n'est pas applicable aux données dont la conservation est spécifiquement exigée par la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication ([1]) aux fins visées à l'article 1er, paragraphe 1, de ladite directive.

▼M2

1 *ter*. Les fournisseurs établissent, sur la base des dispositions nationales adoptées au titre du paragraphe 1, des procédures internes permettant de répondre aux demandes d'accès aux données à caractère personnel concernant les utilisateurs. Ils mettent, sur demande, à la disposition de l'autorité nationale compétente des informations sur ces procédures, sur le nombre de demandes reçues, sur la base juridique invoquée et sur leur réponse.

▼B

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.

([1]) JO L 105 du 13.4.2006, p. 54.

▼M2

Article 15 bis

Mise en œuvre et contrôle de l'application

1. Les États membres déterminent le régime des sanctions, y compris des sanctions pénales s'il y a lieu, applicables aux violations des dispositions nationales prises en application de la présente directive et prennent toute mesure nécessaire pour assurer la mise en œuvre de celles-ci. Les sanctions ainsi prévues doivent être effectives, proportionnées et dissuasives et peuvent être appliquées pour couvrir la durée de l'infraction, même si celle-ci a été ultérieurement corrigée. Les États membres notifient ces dispositions à la Commission, au plus tard le 25 mai 2011, et toute modification ultérieure les concernant dans les meilleurs délais.

2. Sans préjudice de tout recours judiciaire qui pourrait être disponible, les États membres veillent à ce que l'autorité nationale compétente et, le cas échéant, d'autres organismes nationaux aient le pouvoir d'ordonner la cessation des infractions visées au paragraphe 1.

3. Les États membres veillent à ce que l'autorité nationale compétente et, le cas échéant, d'autres organismes nationaux disposent des pouvoirs d'enquête et des ressources nécessaires, et notamment du pouvoir d'obtenir toute information pertinente dont ils pourraient avoir besoin, afin de surveiller et de contrôler le respect des dispositions nationales adoptées en application de la présente directive.

4. Les autorités réglementaire nationales compétentes peuvent adopter des mesures afin d'assurer une coopération transfrontalière effective dans le contrôle de l'application des législations nationales adoptées en application de la présente directive et de créer des conditions harmonisées pour la fourniture de services impliquant des flux de données transfrontaliers.

Les autorités réglementaires nationales fournissent à la Commission, en temps utile avant l'adoption de ces mesures, un résumé des raisons sur lesquelles se fondent leur intervention, les mesures envisagées et la démarche proposée. Après avoir examiné ces informations et consulté l'ENISA et 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, la Commission peut émettre des commentaires ou faire des recommandations, en particulier pour garantir que les mesures envisagées ne font pas obstacle au fonctionnement du marché intérieur. Les autorités réglementaires nationales tiennent le plus grand compte des commentaires ou recommandations de la Commission lorsqu'elles statuent sur ces mesures.

▼B

Article 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.

▼B

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 États 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.

Article 17

Transposition

1. Les États 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.

Lorsque les États 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 États membres.

2. Les États 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.

Article 18

Réexamen

Au plus tard trois ans après la date visée à l'article 17, paragraphe 1, 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 États 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.

Article 19

Abrogation

La directive 97/66/CE est abrogée avec effet à partir de la date visée à l'article 17, paragraphe 1.

Les références faites à la directive abrogée s'entendent comme étant faites à la présente directive.

▼B

Article 20

Entrée en vigueur

La présente directive entre en vigueur le jour de sa publication au *Journal officiel des Communautés européennes*.

Article 21

Destinataires

Les États membres sont destinataires de la présente directive.