COM (2017) 10 final

ASSEMBLÉE NATIONALE

QUATORZIEME LÉGISLATURE

SÉNAT

SESSION ORDINAIRE DE 2016-2017

Reçu à la Présidence de l'Assemblée nationale
le 15 février 2017

Enregistré à la Présidence du Sénat
le 15 février 2017

TEXTE SOUMIS EN APPLICATION DE L'ARTICLE 88-4 DE LA CONSTITUTION

PAR LE GOUVERNEMENT,

À L'ASSEMBLÉE NATIONALE ET AU SÉNAT.

Proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement «vie privée et communications électroniques»)

E 11853

Conseil de
l'Union européenne

Bruxelles, le 16 janvier 2017
(OR. en)

5358/17

Dossier interinstitutionnel:
2017/0003 (COD)

TELECOM 12
COMPET 32
MI 45
DATAPROTECT 4
CONSOM 19
JAI 40
DIGIT 10
FREMP 3
CYBER 10
IA 12
CODEC 52

PROPOSITION

Origine:	Pour le Secrétaire général de la Commission européenne, Monsieur Jordi AYET PUIGARNAU, Directeur
Date de réception:	12 janvier 2017
Destinataire:	Monsieur Jeppe TRANHOLM-MIKKELSEN, Secrétaire général du Conseil de l'Union européenne
N° doc. Cion:	COM(2017) 10 final
Objet:	Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement "vie privée et communications électroniques")

Les délégations trouveront ci-joint le document COM(2017) 10 final.

p.j.: COM(2017) 10 final

COMMISSION
EUROPÉENNE

Bruxelles, le 10.1.2017
COM(2017) 10 final

2017/0003 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement «vie privée et communications électroniques»)

(Texte présentant de l'intérêt pour l'EEE)

{SWD(2017) 3 final}
{SWD(2017) 4 final}
{SWD(2017) 5 final}
{SWD(2017) 6 final}

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

1.1. Justification et objectifs de la proposition

L'un des objectifs de la stratégie pour un marché unique numérique (ci-après la «**stratégie MUN**»)[1] est de faire en sorte que les services numériques soient plus sûrs et suscitent davantage la confiance. À cette fin, la réforme du cadre en matière de protection des données et, en particulier, l'adoption du règlement (UE) 2016/679 ou règlement général sur la protection des données (ci-après le «**RGPD**»)[2] ont été déterminantes. Dans la stratégie MUN, la Commission annonçait également le réexamen de la directive 2002/58/CE (ci-après la «**directive "vie privée et communications électroniques"**»)[3] afin de fournir un niveau élevé de protection de la vie privée aux utilisateurs des services de communications électroniques, et des conditions de concurrence équitables à tous les acteurs économiques. La présente proposition consiste à réexaminer la directive «vie privée et communications électroniques» en anticipant sur les objectifs de la stratégie MUN et en veillant à la conformité au RGPD.

La directive «vie privée et communications électroniques» assure la protection des libertés et droits fondamentaux, en particulier le respect de la vie privée, la confidentialité des communications et la protection des données à caractère personnel dans le secteur des communications électroniques. Elle garantit aussi la libre circulation des données, équipements et services de communications électroniques dans l'Union. Elle transpose en droit dérivé de l'Union le droit fondamental au respect de la vie privée, en ce qui concerne les communications, tel qu'il est consacré à l'article 7 de la Charte des droits fondamentaux de l'Union européenne (ci-après la «**Charte**»).

Conformément aux exigences relatives au «mieux légiférer», la Commission a effectué une évaluation *ex post*, au titre du programme pour une réglementation affûtée et performante (ci-après «**évaluation REFIT**»), de la directive «vie privée et communications électroniques». Il ressort de cette évaluation que les objectifs et les principes du cadre actuel restent valables. Toutefois, depuis la dernière révision de la directive en 2009, d'importantes évolutions technologiques et économiques se sont produites sur le marché. Particuliers et entreprises recourent de plus en plus, pour leurs communications interpersonnelles, à de nouveaux services sur Internet, comme la voix sur IP, la messagerie instantanée et le courrier électronique Web, au lieu des services de communication traditionnels. Ces services de communication par contournement (ci-après «**OTT**») ne sont en général pas soumis au cadre réglementaire actuel de l'Union en matière de communications électroniques, notamment à la directive «vie privée et communications électroniques». En conséquence, celle-ci a été

---

1 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions – Stratégie pour un marché unique numérique en Europe, COM(2015) 192 final.

2 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

3 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).

dépassée par l'évolution technologique avec, pour résultat, que les communications établies par l'intermédiaire de nouveaux services ne sont pas protégées.

1.2. Cohérence avec les dispositions existantes dans le domaine d'action

La présente proposition constitue une *lex specialis* par rapport au RGPD, qu'elle précisera et complétera en ce qui concerne les données de communications électroniques qui peuvent être considérées comme des données à caractère personnel. Toutes les matières relatives au traitement de ces données, qui ne sont pas spécifiquement couvertes par la proposition, le sont par le RGPD. L'harmonisation avec le RGPD a entraîné l'abrogation de certaines dispositions comme les obligations en matière de sécurité figurant à l'article 4 de la directive «vie privée et communications électroniques».

1.3. Cohérence avec les autres politiques de l'Union

La directive «vie privée et communications électroniques» est un élément du cadre réglementaire des communications électroniques. En 2016, la Commission a adopté la proposition de directive établissant le code des communications électroniques européen (ci-après le «**CCEE**»)[4], lequel constitue une révision du cadre. Même si la présente proposition ne fait pas partie intégrante du CCEE, elle repose partiellement sur les définitions qu'il contient, notamment celle des «services de communications électroniques». À l'instar du CCEE, la présente proposition fait aussi entrer les fournisseurs de services OTT dans son champ d'application afin de refléter la réalité du marché. En outre, le CCEE complète la présente proposition en garantissant la sécurité des services de communications électroniques.

La directive 2014/53/UE sur les équipements radioélectriques (ci-après la «**DER**»)[5] instaure un marché unique desdits équipements. En particulier, elle pose comme exigence que les équipements radioélectriques doivent, avant leur mise sur le marché, comporter des garanties afin d'assurer la protection des données à caractère personnel et de la vie privée des utilisateurs. En vertu de la DER et du règlement (UE) n° 1025/2012 relatif à la normalisation européenne[6], la Commission est habilitée à adopter des mesures. La présente proposition n'a pas d'incidence sur la DER.

La proposition ne comporte aucune disposition spécifique à la conservation des données. Elle préserve l'esprit de l'article 15 de la directive «vie privée et communications électroniques» et en harmonise la lettre avec la formulation spécifique de l'article 23 du RGPD, qui précise les motifs permettant aux États membres de limiter la portée des droits et obligations prévus à des articles précis. Par conséquent, les États membres sont libres de maintenir ou de créer, en la matière, des cadres nationaux qui prévoient, entre autres, des mesures de conservation ciblées dans la mesure où ces cadres respectent le droit de l'Union, compte tenu de la jurisprudence

---

4 Proposition de directive du Parlement européen et du Conseil établissant le code des communications électroniques européen (Refonte) [COM(2016) 590 final – 2016/0288(COD)].

5 Directive 2014/53/UE du Parlement européen et du Conseil du 16 avril 2014 relative à l'harmonisation des législations des États membres concernant la mise à disposition sur le marché d'équipements radioélectriques et abrogeant la directive 1999/5/CE (JO L 153 du 22.5.2014, p. 62).

6 Règlement (UE) n° 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision n° 1673/2006/CE du Parlement européen et du Conseil (JO L 316 du 14.11.2012, p. 12).

de la Cour de justice sur l'interprétation de la directive «vie privée et communications électroniques» et de la Charte[7].

Enfin, la proposition ne s'applique pas aux activités des institutions, organes et agences de l'Union. Toutefois, les principes qu'elle contient et certaines obligations concernant le droit au respect de la vie privée et des communications en relation avec le traitement des données de communications électroniques ont été intégrés dans la proposition de règlement abrogeant le règlement (CE) n° 45/2001[8].

2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

2.1. Base juridique

Les articles 16 et 114 du traité sur le fonctionnement de l'Union européenne (ci-après le «**TFUE**») sont les bases juridiques pertinentes pour la proposition.

L'article 16 du TFUE instaure une base juridique spécifique pour l'adoption de règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions de l'Union ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union, et à la libre circulation de ces données. Comme une communication électronique faisant intervenir une personne physique sera en principe considérée comme ayant la nature de données à caractère personnel, la protection des personnes physiques à l'égard de la confidentialité des communications et du traitement de ces données devrait se fonder sur l'article 16.

En outre, la proposition vise à protéger les communications et les intérêts légitimes correspondants des personnes morales. Le droit reconnu à l'article 7 de la Charte doit, conformément à l'article 52, paragraphe 3, de celle-ci, avoir la même interprétation et la même portée que celui énoncé à l'article 8, paragraphe 1, de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (ci-après la «**CEDH**»). En ce qui concerne la portée de l'article 7 de la Charte, la jurisprudence de la Cour de justice de l'Union européenne (ci-après la «**CJUE**»)[9] et de la Cour européenne des droits de l'homme[10] confirme que les activités professionnelles des personnes physiques ne peuvent être exclues de la sauvegarde du droit garanti par l'article 7 de la Charte et l'article 8 de la CEDH.

Étant donné que l'initiative a une double finalité et que le volet concernant la protection des communications des personnes morales et l'objectif de réaliser le marché intérieur de ces communications électroniques et d'assurer son fonctionnement ne peut, à cet égard, être

---

7 Voir affaires jointes C-293/12 et C-594/12 *Digital Rights Ireland et Seitlinger et autres*, ECLI:EU:C:2014:238; affaires jointes C-203/15 et C-698/15 *Tele2 Sverige AB et Secretary of State for the Home Department*, ECLI:EU:C:2016:970.

8 Règlement (CE) n° 45/2001 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 (JO L 8 du 12.1.2001, p. 1).

9 Voir affaire C-450/06 *Varec SA*, ECLI:EU:C:2008:91, point 48.

10 Voir, notamment, CEDH, arrêts *Niemietz c. Allemagne*, 16 décembre 1992, § 29, série A n° 251-B; *Société Colas Est e.a. c. France*, n° 37971/97, § 41, CEDH 2002-III; *Peck c. Royaume-Uni*, n° 44647/98, § 57, CEDH 2003-1; ainsi que *Vinci Construction et GTM Génie Civil et Services c. France*, n° 63629/10 et n° 60567/10, § 63, 2 avril 2015.

considéré comme accessoire, l'initiative devrait donc aussi se fonder sur l'article 114 du TFUE.

2.2. Subsidiarité

Le respect des communications est un droit fondamental reconnu dans la Charte. Le contenu des communications électroniques peut révéler des informations extrêmement sensibles sur les utilisateurs finaux intervenant dans la communication. De même, les métadonnées découlant de communications électroniques peuvent aussi révéler des informations très sensibles et personnelles, comme la CJUE le reconnaît expressément[11]. En majorité, les États membres reconnaissent aussi la nécessité de protéger les communications comme un droit constitutionnel distinct. Même si les États membres ont la possibilité d'adopter des politiques garantissant que ce droit n'est pas enfreint, leur mise en œuvre, faute de règles au niveau de l'Union, ne serait pas uniforme et aboutirait à des restrictions sur les flux transfrontières de données à caractère personnel et non personnel relatives à l'utilisation de services de communications électroniques. Enfin, pour veiller à la concordance avec le RGPD, il est nécessaire de réexaminer la directive «vie privée et communications électroniques» et d'adopter des mesures pour harmoniser les deux instruments.

Les évolutions technologiques et les ambitions affichées dans la stratégie MUN ont renforcé la nécessité d'une action au niveau de l'Union. Le succès de la stratégie MUN dépend du degré d'efficacité avec lequel l'UE brise les niches et les barrières nationales et met à profit les avantages procurés et les économies permises par un marché unique numérique européen. De plus, comme Internet et les technologies numériques ignorent les frontières, le problème ne se limite pas au territoire d'un État membre. Dans la situation actuelle, les États membres sont dans l'impossibilité de résoudre efficacement les problèmes posés. Pour que le marché unique numérique fonctionne correctement, il faut que les opérateurs économiques fournissant des services interchangeables bénéficient de conditions de concurrence équitables, et les utilisateurs finaux d'une protection identique, au niveau de l'Union.

2.3. Proportionnalité

Pour assurer efficacement le respect de la vie privée et des communications par une protection juridique, il est nécessaire d'étendre le champ d'application aux fournisseurs de services OTT. Même si plusieurs de ces fournisseurs, très connus, observent déjà, intégralement ou partiellement, le principe de la confidentialité des communications, la sauvegarde des droits fondamentaux ne peut résulter d'une autorégulation par les entreprises. En outre, protéger efficacement la confidentialité des équipements terminaux revêt une importance accrue car ces équipements sont devenus indispensables, dans le cadre privé comme professionnel, pour stocker des informations sensibles. La mise en œuvre de la directive «vie privée et communications électroniques» ne s'est pas avérée efficace pour ce qui est de responsabiliser l'utilisateur final. Aussi, pour atteindre le but recherché, est-il nécessaire d'appliquer le principe en centralisant le consentement dans des logiciels et en donnant aux utilisateurs des informations sur leurs paramètres de confidentialité. S'agissant de l'application du présent règlement, elle repose sur les autorités de contrôle et le mécanisme de contrôle de la cohérence du RGPD. De plus, la proposition permet aux États membres de prendre des mesures dérogatoires nationales pour des motifs légitimes précis. Par conséquent, la proposition ne va pas au-delà de ce qui est nécessaire pour atteindre ses objectifs et est

[11] Voir note de bas de page 7.

conforme au principe de proportionnalité énoncé à l'article 5 du traité sur l'Union européenne. Les obligations imposées aux services concernés sont le moins contraignantes possible, sans pour autant entamer les droits fondamentaux en question.

2.4. Choix de l'instrument

La Commission présente une proposition de règlement afin d'assurer la conformité au RGPD et de garantir la sécurité juridique aux utilisateurs comme aux entreprises en évitant les divergences d'interprétation dans les États membres. Un règlement permet aux utilisateurs de bénéficier du même niveau de protection dans l'ensemble de l'Union, et aux entreprises actives dans plusieurs pays de supporter des coûts de mise en conformité moins élevés.

3. RÉSULTATS DES ÉVALUATIONS EX POST, DES CONSULTATIONS DES PARTIES INTÉRESSÉES ET DES ANALYSES D'IMPACT

3.1. Évaluations ex post/bilans de qualité de la législation existante

L'évaluation REFIT a consisté à déterminer dans quelle mesure la directive «vie privée et communications électroniques» a permis une protection efficace de la vie privée et de la confidentialité des communications dans l'UE, ainsi qu'à recenser les éventuels doublons.

La conclusion en a été que les objectifs de la directive susmentionnés sont toujours **pertinents**. Tandis que le RGPD garantit la protection des données à caractère personnel, la directive «vie privée et communications électroniques» préserve la confidentialité des communications, lesquelles peuvent aussi contenir des données à caractère non personnel et des données relatives à une personne morale. Par conséquent, un instrument distinct devrait assurer une protection efficace de l'article 7 de la Charte. D'autres dispositions, comme les règles sur l'envoi de communications commerciales non sollicitées, se sont avérées toujours pertinentes également.

En termes d'**efficacité et** d'**efficience**, il est ressorti de l'évaluation REFIT que la directive n'a pas complètement atteint ses objectifs. La formulation confuse de certaines dispositions et l'ambiguïté des concepts juridiques ont nui à l'harmonisation et donc posé des problèmes aux entreprises souhaitant exercer leurs activités dans plusieurs pays. L'évaluation a aussi montré que des dispositions avaient fait peser une charge inutile sur les entreprises et les particuliers. Par exemple, la règle du consentement pour préserver la confidentialité des équipements terminaux n'a pas permis d'atteindre les objectifs poursuivis car l'utilisateur final se voit demander d'accepter des témoins («cookies») traceurs sans savoir ce que c'est et, dans certains cas, s'expose même à ce que des cookies soient installés sans son consentement. Cette règle est à la fois trop inclusive, car elle couvre aussi des pratiques ne portant pas atteinte à la vie privée, et trop exclusive, car elle ne couvre pas expressément certaines techniques de suivi (p. ex. capture d'empreintes numériques) ne consistant pas nécessairement à accéder à des données ou à en stocker dans le dispositif. Enfin, son application peut être coûteuse pour les entreprises.

L'évaluation a permis de conclure que les règles de la directive «vie privée et communications électroniques» procurent toujours une **valeur ajoutée européenne** pour ce qui est de mieux atteindre l'objectif d'assurer le respect de la vie privée en ligne, compte tenu de la dimension de plus en plus transnationale du marché des communications électroniques. Elle a aussi démontré que, globalement, les règles sont **en concordance** avec le reste de la

législation applicable, même si quelques doublons ont été recensés avec le nouveau RGPD (voir à la partie 1.2).

3.2. Consultations des parties intéressées

La Commission a organisé une consultation publique entre le 12 avril et le 5 juillet 2016 et a reçu 421 réponses[12]. Les principales conclusions en sont les suivantes[13]:

– **Nécessité de règles spécifiques au secteur des communications électroniques sur la confidentialité de celles-ci**: 83,4 % des particuliers et des organisations de consommateurs et de la société civile et 88,9 % des pouvoirs publics ayant répondu l'approuvent, tandis que 63,4 % des entreprises participantes la désapprouvent.

– **Extension du champ d'application aux nouveaux services de communication (OTT)**: 76 % des particuliers et des représentants de la société civile et 93,1 % des pouvoirs publics l'approuvent, mais seulement 36,2 % des entreprises participantes y sont favorables.

– **Modification des dérogations concernant le consentement pour le traitement des données de trafic et de localisation**: 49,1 % des particuliers et des organisations de consommateurs et de la société civile et 36 % des pouvoirs publics préfèrent que les dérogations ne soient pas étendues tandis que, du côté des entreprises, 36 % sont favorables à une extension des dérogations et les 2/3 préconisent l'abrogation pure et simple des dispositions.

– **Solutions proposées au problème du consentement pour les cookies**: 81,2 % des particuliers et 63 % des pouvoirs publics soutiennent la solution consistant à imposer aux fabricants d'équipements terminaux l'obligation de commercialiser des produits dotés de paramètres de confidentialité activés par défaut, tandis que 58,3 % des entreprises sont favorables à la solution de l'autorégulation ou de la corégulation.

En outre, la Commission européenne a organisé deux ateliers en avril 2016, l'un ouvert à toutes les parties intéressées et l'autre ouvert aux seules autorités nationales compétentes, afin de traiter les principales questions soulevées par la consultation publique. Les opinions exprimées au cours des ateliers ont reflété les résultats de la consultation publique.

Pour recueillir l'avis des Européens, une enquête Eurobaromètre sur la vie privée et les communications électroniques[14] a été réalisée dans toute l'UE. Les principales conclusions en sont les suivantes[15]:

---

12 162 contributions émanant de particuliers, 33 d'organisations de la société civile et de consommateurs, 186 d'entreprises et 40 de pouvoirs publics, y compris des autorités responsables de l'application de la directive «vie privée et communications électroniques».

13 Le rapport complet (en anglais) est disponible à l'adresse: https://ec.europa.eu/digital-single-market/news-redirect/37204.

14 Enquête Eurobaromètre 443 de 2016 sur la vie privée et les communications électroniques (SMART 2016/079).

15 Le rapport complet (en anglais) est disponible à l'adresse: https://ec.europa.eu/digital-single-market/news-redirect/37205.

– Pour 78 % des personnes interrogées, il est très important qu'on ne puisse accéder aux informations à caractère personnel contenues dans leur ordinateur, leur smartphone ou leur tablette qu'avec leur permission.

– 72 % considèrent comme très important que la confidentialité de leurs courriels et de leur messagerie instantanée en ligne soit garantie.

– 89 % conviennent, comme il a été suggéré, que les paramètres par défaut de leur navigateur devraient empêcher le partage de leurs informations.

3.3. Obtention et utilisation d'expertise

La Commission s'est appuyée sur les conseils avisés suivants:

– consultations ciblées de groupes d'experts de l'UE: avis du groupe de travail «Article 29»; avis du CEPD; avis de la plateforme REFIT; avis de l'ORECE; avis de l'ENISA et de membres du réseau de coopération pour l'application de la législation en matière de protection des consommateurs;

– expertise externe, notamment les deux études suivantes:

  – «*ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation*» (SMART 2013/007116);

  – «*Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector*» (SMART 2016/0080).

3.4. Analyse d'impact

Une analyse d'impact a été réalisée pour la présente proposition et, le 28 septembre 2016, le comité d'examen de la réglementation a émis un avis favorable la concernant[16]. Suivant les recommandations du comité, l'analyse d'impact décrit plus en détail le champ d'application de l'initiative, sa concordance avec les autres instruments juridiques (RGPD, CCEE, DER) et la nécessité d'un instrument distinct. Le scénario de référence est plus élaboré et plus précis. L'analyse des incidences est plus fine et plus équilibrée, avec une description plus claire et plus poussée des coûts et avantages escomptés.

Les options suivantes ont été examinées en fonction des critères d'efficacité, d'efficience et de cohérence:

– **option 1:** mesures non législatives (non contraignantes);

– **option 2:** renforcement limité du respect de la vie privée/confidentialité et simplification;

– **option 3:** renforcement modéré du respect de la vie privée/confidentialité et simplification;

– **option 4:** renforcement important du respect de la vie privée/confidentialité et simplification;

[16] http://ec.europa.eu/transparency/regdoc/?fuseaction=ia.

– **option 5:** abrogation de la directive «vie privée et communications électroniques».

L'**option 3** a été distinguée comme l'**option privilégiée**, sous la plupart des aspects, pour atteindre les objectifs poursuivis, compte tenu notamment de son efficience et de sa cohérence. Ses principaux avantages sont les suivants:

– protection renforcée de la confidentialité des communications électroniques par l'extension du champ d'application de l'instrument juridique à de nouveaux services de communications électroniques fonctionnellement équivalents. En outre, le règlement renforce le contrôle exercé par l'utilisateur final en précisant que le consentement peut être exprimé à l'aide de paramètres techniques appropriés;

– protection renforcée contre les communications non sollicitées par l'instauration de l'obligation de fournir l'identification de la ligne appelante ou d'un indicatif obligatoire pour les appels commerciaux, et par les possibilités accrues de bloquer les appels émanant de numéros indésirables;

– simplification et clarification de l'environnement réglementaire par la réduction de la marge de manœuvre laissée aux États membres, l'abrogation des dispositions obsolètes et l'extension des exceptions aux règles de consentement.

Il est prévu que l'incidence économique de l'option 3 sera globalement proportionnée aux objectifs de la proposition. Elle offre aux services traditionnels de communications électroniques des débouchés commerciaux en matière de traitement des données de communication, tandis que les fournisseurs de services OTT seront assujettis aux mêmes règles, ce qui implique des coûts supplémentaires de mise en conformité pour ces derniers opérateurs. Toutefois, ce changement n'aura pas d'effet significatif sur les services OTT qui fonctionnent déjà sur la base du consentement. Enfin, l'incidence de l'option serait imperceptible dans les États membres qui ont déjà étendu ces règles aux services OTT.

Le fait de centraliser le consentement dans des logiciels comme les navigateurs Internet, d'inviter les utilisateurs à choisir leurs paramètres de confidentialité et d'étendre les exceptions à la règle du consentement pour les cookies donnerait à une grande partie des entreprises la possibilité de se débarrasser des bandeaux et avis en la matière et conduirait donc à des économies de coûts et une simplification potentiellement importantes. Toutefois, il sera peut-être plus difficile aux annonceurs en ligne pratiquant le ciblage d'obtenir un consentement si une forte proportion d'utilisateurs choisit le paramètre «refuser les cookies de tiers». En même temps, centraliser le consentement ne prive pas les exploitants de sites Web de la possibilité d'obtenir un consentement par l'envoi de demandes individuelles aux utilisateurs finaux et donc de conserver leur modèle économique actuel. Il s'ensuivrait des coûts supplémentaires pour certains fournisseurs de navigateurs ou de logiciels similaires car ils devraient garantir des paramètres respectueux de la vie privée.

L'étude externe a permis de définir trois scénarios distincts de mise en œuvre de l'option 3 en fonction de l'entité qui établira la boîte de dialogue entre l'utilisateur qui a choisi les paramètres «refuser les cookies de tiers» ou «ne pas pister» et les sites Web visités qui souhaitent que l'internaute revienne sur son choix. Les entités qui pourraient être chargées de cette tâche technique sont: 1) des logiciels comme les navigateurs Internet; 2) le traceur tiers; 3) chaque site Web (c.-à-d. le service de la société de l'information demandé par l'utilisateur). Par rapport au scénario de référence, l'option 3 permettrait de réaliser des économies globales, en termes de coûts de mise en conformité, de 70 % (948,8 millions d'EUR d'économies)

selon le premier scénario (solution des navigateurs), retenu dans la présente proposition. Les économies seraient moindres selon les autres scénarios. Comme les économies globales sont dues, dans une large mesure, à une diminution très importante du nombre d'entreprises concernées, le montant individuel des coûts de mise en conformité qu'une entreprise devrait supporter, en moyenne, serait plus élevé qu'aujourd'hui.

3.5. Réglementation affûtée et simplification

Les mesures politiques proposées au titre de l'option privilégiée permettent d'atteindre l'objectif de simplification et de réduction de la charge administrative, conformément aux conclusions de l'évaluation REFIT et à l'avis de la plateforme REFIT[17].

La plateforme REFIT a formulé trois séries de recommandations à l'intention de la Commission:

– Il conviendrait de mieux protéger la vie privée des personnes en harmonisant la directive «vie privée et communications électroniques» et le règlement général sur la protection des données.

– Il conviendrait de protéger plus efficacement les personnes contre la prospection non sollicitée en prévoyant des exceptions à la règle du consentement pour les cookies.

– La Commission traite les problèmes de mise en œuvre nationale et facilite l'échange de bonnes pratiques entre États membres.

La proposition prévoit expressément:

– l'utilisation de définitions neutres du point de vue technologique pour englober de nouveaux services et technologies et assurer la pérennité du règlement;

– l'abrogation des règles de sécurité pour supprimer les doublons réglementaires;

– la clarification du champ d'application pour éliminer/réduire le risque de divergence dans la mise en œuvre par les États membres (point 3 de l'avis);

– la clarification et la simplification de la règle du consentement pour l'utilisation des cookies et autres identificateurs, comme exposé aux parties 3.1 et 3.4 (point 2 de l'avis);

– la convergence des autorités de contrôle avec les autorités responsables de l'application du RGPD et le recours au mécanisme de cohérence du RGPD.

3.6. Incidence sur les droits fondamentaux

La proposition vise à rendre plus efficace la protection de la vie privée et des données à caractère personnel traitées en relation avec les communications électroniques et à en relever le niveau, conformément aux articles 7 et 8 de la Charte, et à procurer une plus grande sécurité juridique. La proposition complète et précise le RGPD. Préserver efficacement la confidentialité des communications est essentiel à l'exercice de la liberté d'expression et

[17] http://ec.europa.eu/smart-regulation/refit/refit-platform/docs/recommendations/opinion_comm_net.pdf.

d'information et à d'autres droits apparentés tels que le droit à la protection des données à caractère personnel ou la liberté de pensée, de conscience et de religion.

4. INCIDENCE BUDGÉTAIRE

La proposition n'a aucune incidence sur le budget de l'Union.

5. AUTRES ÉLÉMENTS

5.1. Plans de mise en œuvre et modalités de suivi, d'évaluation et d'information

La Commission supervisera l'application du règlement et présentera tous les trois ans un rapport sur son évaluation au Parlement européen, au Conseil et au Comité économique et social européen. Ces rapports seront publiés et décriront en détail comment le présent règlement est appliqué et exécuté dans les faits.

5.2. Explication détaillée des différentes dispositions de la proposition

Le chapitre I contient les dispositions générales: l'objet (article 1er), le champ d'application (articles 2 et 3) et ses définitions, y compris les références aux définitions pertinentes tirées d'autres instruments de l'UE comme le RGPD.

Le chapitre II contient les principales dispositions assurant la confidentialité des communications électroniques (article 5) et précise à quelles fins et conditions limitées le traitement de ces données de communication est permis (articles 6 et 7). Il traite aussi de la protection des équipements terminaux (i) en garantissant l'intégrité des informations qui y sont stockées et (ii) en protégeant les informations émises à partir de ceux-ci, car elles peuvent permettre d'identifier leur utilisateur final (article 8). Enfin, l'article 9 détaille la notion de consentement de l'utilisateur final, motif légal central du présent règlement, en renvoyant expressément à sa définition et aux conditions prévues par le RGPD, tandis que l'article 10 impose aux fournisseurs de logiciels permettant des communications électroniques l'obligation d'aider l'utilisateur final à choisir efficacement ses paramètres de confidentialité. L'article 11 précise à quelles fins et conditions les États membres peuvent restreindre l'application des dispositions ci-dessus.

Le chapitre III concerne les droits de l'utilisateur final de contrôler l'envoi et la réception de communications électroniques pour protéger sa vie privée: (i) le droit de l'utilisateur final d'empêcher la présentation de l'identification de la ligne appelante pour préserver son anonymat (article 12), et ses restrictions (article 13); et (ii) l'obligation, pour les fournisseurs de services de communications interpersonnelles fondés sur la numérotation et accessibles au public, d'offrir la possibilité de limiter la réception des appels indésirables (article 14). Ce chapitre régit aussi les conditions auxquelles il est possible de faire figurer l'utilisateur final dans des annuaires accessibles au public (article 15) et les conditions auxquelles il est possible d'effectuer des communications non sollicitées pour la prospection directe (article 17). Il concerne également les risques pour la sécurité et prévoit l'obligation, pour les fournisseurs de services de communications électroniques, d'alerter l'utilisateur final en cas de risque particulier pouvant compromettre la sécurité des réseaux et services. Les obligations en matière de sécurité figurant dans le RGPD et le CCEE s'appliqueront aux fournisseurs de services de communications électroniques.

Le chapitre IV est consacré à la supervision et au contrôle de l'application du présent règlement, confiés aux autorités de contrôle responsables du RGPD eu égard aux fortes synergies entre les questions générales de protection des données et la confidentialité des communications (article 18). Les pouvoirs du comité européen de la protection des données sont étendus (article 19) et le mécanisme de coopération et de cohérence prévu au titre du RGPD s'appliquera en cas de problème transfrontière relatif au présent règlement (article 20).

Le chapitre V détaille les divers recours dont dispose l'utilisateur final (articles 21 et 22) ainsi que les sanctions qui peuvent être infligées (article 24), notamment les conditions générales pour infliger des amendes administratives (article 23).

Le chapitre VI concerne l'adoption d'actes délégués et d'exécution conformément aux articles 290 et 291 du traité.

Enfin, la chapitre VII contient les dispositions finales du présent règlement: l'abrogation de la directive «vie privée et communications électroniques», le suivi et le réexamen, l'entrée en vigueur et la mise en application. Concernant le réexamen, la Commission entend établir notamment si un acte juridique distinct reste nécessaire à la lumière des évolutions juridiques, techniques ou économiques et compte tenu de la première évaluation du règlement (UE) 2016/679 qui doit avoir lieu d'ici au 25 mai 2020.

2017/0003 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement «vie privée et communications électroniques»)

(Texte présentant de l'intérêt pour l'EEE)

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment ses articles 16 et 114,

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen[1],

vu l'avis du Comité des régions[2],

vu l'avis du Contrôleur européen de la protection des données[3],

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

(1) L'article 7 de la Charte des droits fondamentaux de l'Union européenne (ci-après la «Charte») consacre le droit fondamental de toute personne au respect de sa vie privée et familiale, de son domicile et de ses communications. Le respect de la confidentialité des communications d'une personne est une dimension essentielle de ce droit. La confidentialité des communications électroniques garantit que les informations échangées entre les parties ainsi que les éléments extérieurs à la communication, y compris ceux indiquant quand, d'où et à qui les informations ont été envoyées, ne sont divulguées à personne d'autre que les parties intervenant dans la communication. Le principe de confidentialité devrait s'appliquer aux moyens de communication actuels et futurs, y compris la téléphonie vocale, l'accès à Internet, les applications de messagerie instantanée, le courrier électronique, les appels téléphoniques par Internet et la messagerie personnelle fournie par les réseaux sociaux.

1 JO C du , p. .
2 JO C du , p. .
3 JO C du , p. .

(2) Le contenu des communications électroniques peut révéler des informations extrêmement sensibles sur les personnes physiques intervenant dans la communication, depuis leurs expériences personnelles et émotions jusqu'à leurs problèmes de santé, préférences sexuelles et opinions politiques, dont la divulgation pourrait causer un préjudice personnel ou social, des pertes économiques ou un embarras. De même, les métadonnées découlant de communications électroniques peuvent aussi révéler des informations très sensibles et personnelles. Ces métadonnées comprennent les numéros appelés, les sites Web visités, le lieu, la date, l'heure et la durée des appels passés par un individu, etc., qui permettent de tirer des conclusions précises sur la vie privée des personnes intervenant dans la communication électronique, comme leurs rapports sociaux, leurs habitudes et activités au quotidien, leurs intérêts, leurs goûts, etc.

(3) Les données de communications électroniques peuvent aussi révéler des informations concernant les personnes morales, telles que des secrets d'affaires ou d'autres informations sensibles ayant une valeur économique. Aussi les dispositions du présent règlement devraient-elles s'appliquer à la fois aux personnes physiques et aux personnes morales. De plus, le présent règlement devrait garantir que les dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil[4] s'appliquent aussi aux utilisateurs finaux qui sont des personnes morales. Cela comprend la définition du consentement en vertu du règlement (UE) 2016/679. C'est cette définition qui devrait s'appliquer lorsqu'il est fait référence au consentement d'un utilisateur final, y compris d'une personne morale. En outre, les personnes morales devraient avoir les mêmes droits que les utilisateurs finaux qui sont des personnes physiques en ce qui concerne les autorités de contrôle, lesquelles devraient aussi, en vertu du présent règlement, être responsables du suivi de son application relativement aux personnes morales.

(4) Conformément à l'article 8, paragraphe 1, de la Charte et à l'article 16, paragraphe 1, du traité sur le fonctionnement de l'Union européenne, toute personne a droit à la protection des données à caractère personnel la concernant. Le règlement (UE) 2016/679 définit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la libre circulation de ces données. Les données de communications électroniques peuvent comporter des données à caractère personnel telles que définies dans le règlement (UE) 2016/679.

(5) Les dispositions du présent règlement précisent et complètent les règles générales de protection des données à caractère personnel définies dans le règlement (UE) 2016/679 en ce qui concerne les données de communications électroniques qui peuvent être considérées comme des données à caractère personnel. Le présent règlement n'abaisse donc pas le niveau de protection dont bénéficient les personnes physiques en vertu du règlement (UE) 2016/679. Le traitement des données de communications électroniques par les fournisseurs de services de communications électroniques ne devrait être permis que conformément au présent règlement.

[4] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

(6) Même si les principes et dispositions majeures de la directive 2002/58/CE du Parlement européen et du Conseil[5] restent en général valables, celle-ci a en partie été dépassée par l'évolution des technologies et du marché avec, pour résultat, des incohérences ou des insuffisances dans la protection effective de la vie privée et de la confidentialité, en relation avec les communications électroniques. Cette évolution se traduit notamment par l'arrivée sur le marché de services de communications électroniques qui, du point de vue du consommateur, peuvent se substituer aux services traditionnels, mais qui ne sont pas soumis au même ensemble de règles. Un autre aspect en est l'émergence de nouvelles techniques qui permettent de suivre le comportement en ligne de l'utilisateur final, mais qui ne sont pas couvertes par la directive 2002/58/CE. Celle-ci devrait donc être abrogée et remplacée par le présent règlement.

(7) Les États membres devraient être autorisés, dans les limites du présent règlement, à maintenir ou instaurer des dispositions nationales pour préciser davantage les règles qu'il contient et leur mise en œuvre, afin d'en garantir une application et une interprétation efficaces. Par conséquent, la marge d'appréciation dont les États membres disposent à cet égard devrait leur permettre de préserver un équilibre entre la protection de la vie privée et des données à caractère personnel et la libre circulation des données de communications électroniques.

(8) Le présent règlement devrait s'appliquer aux fournisseurs de services de communications électroniques, aux fournisseurs d'annuaires accessibles au public et aux fournisseurs de logiciels permettant des communications électroniques, y compris la récupération et la présentation d'informations sur Internet. Il devrait également s'appliquer aux personnes physiques et morales utilisant des services de communications électroniques pour envoyer des communications commerciales de prospection directe ou recueillir des informations qui concernent l'équipement terminal de l'utilisateur final ou qui y sont stockées.

(9) Le présent règlement devrait s'appliquer aux données de communications électroniques traitées en relation avec la fourniture et l'utilisation de services de communications électroniques dans l'Union, que le traitement ait lieu ou non dans l'Union. De plus, afin que les utilisateurs finaux dans l'Union ne soient pas privés d'une protection efficace, le présent règlement devrait également s'appliquer aux données de communications électroniques traitées en relation avec la fourniture de services de communications électroniques de l'extérieur de l'Union à des utilisateurs finaux à l'intérieur de l'Union.

(10) Les équipements radioélectriques et leurs logiciels, qui sont mis sur le marché intérieur de l'Union, doivent être conformes à la directive 2014/53/UE du Parlement européen et du Conseil[6]. Le présent règlement ne devrait avoir d'incidence sur l'applicabilité d'aucune des exigences de cette directive, ni sur le pouvoir de la Commission d'adopter, conformément à celle-ci, des actes délégués exigeant que

---

[5] 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).

[6] Directive 2014/53/UE du Parlement européen et du Conseil du 16 avril 2014 relative à l'harmonisation des législations des États membres concernant la mise à disposition sur le marché d'équipements radioélectriques et abrogeant la directive 1999/5/CE (JO L 153 du 22.5.2014, p. 62).

certaines catégories ou classes d'équipements radioélectriques comportent des garanties afin d'assurer la protection des données à caractère personnel et de la vie privée des utilisateurs finaux.

(11) Les services utilisés à des fins de communication et les moyens techniques de leur fourniture ont considérablement évolué. Les utilisateurs finaux délaissent de plus en plus les services traditionnels de téléphonie vocale, de messages courts (SMS) et d'acheminement de courrier électronique au profit de services en ligne fonctionnellement équivalents comme la voix sur IP, les services de messagerie et de courrier électronique Web. Afin que les utilisateurs finaux recourant à des services fonctionnellement équivalents bénéficient d'une protection efficace et identique, le présent règlement reprend la définition des services de communications électroniques figurant dans la [directive du Parlement européen et du Conseil établissant le code des communications électroniques européen[7]]. Cette définition englobe non seulement les services d'accès à Internet et les services consistant entièrement ou partiellement en la transmission de signaux, mais aussi les services de communications interpersonnelles, fondés ou non sur la numérotation, comme par exemple la voix sur IP, les services de messagerie et de courrier électronique Web. Préserver la confidentialité des communications est également essentiel en ce qui concerne les services de communications interpersonnelles qui sont accessoires à un autre service. Par conséquent, ce type de services ayant aussi une fonction de communication devrait être couvert par le présent règlement.

(12) Les dispositifs et machines connectés communiquent de plus en plus entre eux à l'aide des réseaux de communications électroniques (Internet des objets). L'établissement de communications de machine à machine implique la transmission de signaux sur un réseau et, partant, constitue un service de communications électroniques. Afin d'assurer la sauvegarde totale des droits au respect de la vie privée et à la confidentialité des communications, et de promouvoir un Internet des objets fiable et sûr dans le marché unique numérique, il est nécessaire de préciser que le présent règlement devrait s'appliquer à l'établissement des communications de machine à machine. Par conséquent, ces communications devraient aussi être soumises au principe de confidentialité inscrit dans le présent règlement. Des garanties spécifiques pourraient également être adoptées en vertu d'une législation sectorielle comme, par exemple, la directive 2014/53/UE.

(13) Le développement de technologies sans fil rapides et efficaces a contribué à ce que, de plus en plus, un accès à Internet soit disponible au public par l'intermédiaire de réseaux sans fil, ouverts à tous dans des espaces publics ou semi-privés, comme les bornes Wi-Fi situées à différents endroits des villes, grands magasins, centres commerciaux et hôpitaux. Dans la mesure où ces réseaux de communications sont fournis à un groupe indéfini d'utilisateurs finaux, la confidentialité des communications établies par de tels réseaux devrait être préservée. Le fait que des services de communications électroniques sans fil puissent être accessoires à d'autres services ne devrait pas faire obstacle à la préservation de la confidentialité des données de communication ni à l'application du présent règlement. Par conséquent, celui-ci devrait s'appliquer aux données de communications électroniques utilisant des

[7] Proposition de directive du Parlement européen et du Conseil établissant le code des communications électroniques européen (Refonte) [COM(2016) 590 final – 2016/0288(COD)].

services de communications électroniques et des réseaux de communications publics. En revanche, il ne devrait pas s'appliquer aux groupes fermés d'utilisateurs finaux comme les réseaux d'entreprise dont l'accès est limité aux personnes faisant partie de la société.

(14) Les données de communications électroniques devraient être définies de façon suffisamment large et neutre du point de vue technologique pour englober toute information concernant le contenu transmis ou échangé (contenu des communications électroniques) et toute information concernant l'utilisateur final de services de communications électroniques traitée aux fins de la transmission, la distribution ou l'échange de ce contenu, y compris les données permettant de retracer une communication et d'en déterminer l'origine et la destination ainsi que le lieu, la date, l'heure, la durée et le type. Indépendamment du fait que les signaux et les données correspondantes soient transmis par des moyens filaires, radioélectriques, optiques ou électromagnétiques, y compris les réseaux satellitaires, les réseaux câblés, les réseaux hertziens fixes (à commutation de circuits et de paquets, y compris Internet) et mobiles ou les systèmes utilisant le réseau électrique, les données associées à ces signaux devraient être considérées comme des métadonnées de communications électroniques et donc être soumises aux dispositions du présent règlement. Les informations concernant l'abonnement au service, lorsqu'elles sont traitées aux fins de la transmission, la distribution ou l'échange du contenu des communications électroniques, peuvent constituer de telles métadonnées.

(15) Les données de communications électroniques devraient être traitées comme des données confidentielles. Cela signifie que toute interférence avec leur transmission, soit directement par intervention humaine, soit indirectement par traitement automatisé, sans le consentement de toutes les parties communicantes, devrait être interdite. L'interdiction de l'interception des données de communication devrait s'appliquer durant leur acheminement, c'est-à-dire jusqu'à la réception du contenu de la communication électronique par le destinataire. L'interception de données de communications électroniques peut se produire, par exemple, lorsqu'une personne, autre que les parties communicantes, écoute des appels, lit, balaye ou stocke le contenu de communications électroniques, ou les métadonnées associées, à des fins autres que l'échange de communications. Il y a également interception lorsque des tiers contrôlent les sites Web visités, le calendrier des visites, l'interaction avec autrui, etc., sans le consentement de l'utilisateur final concerné. Comme la technologie évolue, les moyens techniques de procéder à une interception se sont multipliés. Il peut s'agir de l'installation de matériel qui recueille des données des équipements terminaux sur des zones ciblées, comme les intercepteurs d'identité internationale d'abonné mobile (ou «IMSI catchers»), ou de programmes et techniques qui permettent, par exemple, de contrôler subrepticement les habitudes de navigation aux fins de la création de profils d'utilisateur final. Il y a d'autres exemples d'interception comme la capture, à partir de réseaux ou de routeurs sans fil non cryptés, de données de charge utile ou de contenu, y compris des habitudes de navigation, sans le consentement de l'utilisateur final.

(16) L'interdiction du stockage des communications ne vise pas à empêcher le stockage automatique, intermédiaire et transitoire de ces informations tant que celui-ci a lieu à la seule fin de permettre la transmission dans le réseau de communications électroniques. Elle ne devrait pas empêcher le traitement des données de communications électroniques pour assurer la sécurité et la continuité des services de

communications électroniques, notamment en recensant les menaces pour la sécurité comme la présence de logiciel malveillant, ni le traitement des métadonnées pour répondre aux exigences en matière de qualité de service, comme la latence, la gigue, etc.

(17) Le traitement des données de communications électroniques peut être utile aux entreprises, aux consommateurs et à la société dans son ensemble. Par rapport à la directive 2002/58/CE, le présent règlement donne aux fournisseurs de services de communications électroniques davantage de possibilités de traiter les métadonnées de communications électroniques, sur la base du consentement des utilisateurs finaux. Toutefois, ceux-ci attachent une grande importance à la confidentialité de leurs communications, y compris de leurs activités en ligne, et au fait de vouloir contrôler l'utilisation des données de communications électroniques à des fins autres que l'établissement de la communication. Par conséquent, le présent règlement devrait exiger des fournisseurs de services de communications électroniques qu'ils obtiennent le consentement des utilisateurs finaux pour traiter des métadonnées de communications électroniques, y compris les données de localisation du dispositif générées afin de donner accès et maintenir la connexion au service. Les données de localisation qui sont générées dans un contexte autre que celui de la fourniture de services de communications électroniques ne devraient pas être considérées comme des métadonnées. Comme exemple d'utilisation commerciale de métadonnées de communications électroniques par des fournisseurs de services de communications électroniques, on peut citer la fourniture de cartes de densité de clics, représentation graphique de données à l'aide de couleurs pour indiquer la présence d'individus. Pour afficher les mouvements de trafic dans certaines directions au cours d'une période de temps déterminée, un identificateur est nécessaire pour relier les positions des individus à des intervalles de temps donnés. Si l'on devait utiliser des données anonymes, on ne disposerait pas de cet identificateur et les mouvements ne pourraient pas être visualisés. Une telle utilisation des métadonnées de communications électroniques pourrait, par exemple, permettre aux pouvoirs publics et aux exploitants de transports publics de déterminer où développer de nouvelles infrastructures en fonction de l'usage des structures existantes et de la pression que celles-ci subissent. Lorsqu'un type de traitement des métadonnées de communications électroniques, notamment à l'aide de nouvelles technologies, est susceptible, compte tenu de la nature, de la portée, du contexte et de la finalité du traitement, de présenter un risque élevé pour les droits et libertés de personnes physiques, il convient de procéder à une analyse d'impact relative à la protection des données et, le cas échéant, de consulter l'autorité de contrôle préalablement au traitement, conformément aux articles 35 et 36 du règlement (UE) 2016/679.

(18) L'utilisateur final peut consentir au traitement de ses métadonnées afin de bénéficier de services spécifiques comme des services de protection contre les activités frauduleuses (par l'analyse en temps réel des données d'utilisation et de localisation et du compte client). Dans l'économie numérique, les services sont souvent fournis moyennant une contrepartie non pécuniaire, par exemple l'exposition de l'utilisateur final aux publicités. Aux fins du présent règlement, le consentement de l'utilisateur final, que celui-ci soit une personne physique ou morale, devrait avoir le même sens et être soumis aux mêmes conditions que le consentement de la personne concernée en vertu du règlement (UE) 2016/679. L'accès Internet à haut débit de base et les services de communications vocales doivent être considérés comme des services essentiels pour que les individus puissent communiquer et bénéficier des avantages de

l'économie numérique. Le consentement relatif au traitement de données résultant de l'utilisation d'Internet ou des communications vocales ne sera pas valable si la personne concernée ne dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice.

(19) Le contenu des communications électroniques relève intrinsèquement du droit fondamental au respect de la vie privée et familiale, du domicile et des communications sauvegardé en vertu de l'article 7 de la Charte. Une interférence avec le contenu des communications électroniques ne devrait être autorisée que dans des conditions très clairement définies, à des fins précises et sous réserve de garanties adéquates contre les abus. Le présent règlement prévoit la possibilité, pour les fournisseurs de services de communications électroniques, de traiter des données de communications électroniques en transit, avec le consentement éclairé de tous les utilisateurs finaux concernés. Par exemple, les fournisseurs peuvent proposer des services qui impliquent le balayage des courriels pour en supprimer certain matériel prédéfini. Étant donné la sensibilité du contenu des communications, le présent règlement établit la présomption selon laquelle le traitement de données relatives à un tel contenu présentera des risques élevés pour les droits et libertés des personnes physiques. Lors du traitement de ce type de données, le fournisseur du service de communications électroniques devrait toujours consulter l'autorité de contrôle au préalable et ce, conformément à l'article 36, paragraphes 2 et 3, du règlement (UE) 2016/679. La présomption ne s'applique pas au traitement de données relatives au contenu destiné à fournir un service demandé par l'utilisateur final lorsque celui-ci a consenti audit traitement et que ce dernier est effectué aux fins et pour une durée strictement nécessaires et proportionnées à un tel service. Après que le contenu des communications électroniques a été envoyé par l'expéditeur et reçu par le ou les destinataire(s), il peut être enregistré ou stocké par l'utilisateur final, les utilisateurs finaux ou un tiers chargé par ceux-ci d'enregistrer ou de stocker de telles données. Tout traitement de ces données doit être conforme au règlement (UE) 2016/679.

(20) L'équipement terminal de l'utilisateur final de réseaux de communications électroniques et toute information relative à l'utilisation de cet équipement, en particulier qu'elle y soit stockée, qu'elle soit émise par l'équipement, demandée à celui-ci ou traitée afin de lui permettre de se connecter à un autre dispositif et/ou équipement de réseau, font partie de la sphère privée de l'utilisateur final nécessitant une protection en vertu de la Charte des droits fondamentaux de l'Union européenne et de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. Étant donné qu'un tel équipement contient ou traite des informations qui peuvent fournir des détails sur la complexité émotionnelle, politique et sociale d'un individu, qu'il s'agisse du contenu des communications, des images, de la localisation de l'individu par l'accès aux fonctionnalités GPS du dispositif, des listes de contacts et d'autres informations déjà stockées dans le dispositif, les informations relatives à cet équipement exigent une protection renforcée de la vie privée. De plus, ce que l'on appelle les logiciels espions, pixels invisibles, identificateurs cachés, cookies traceurs et autres outils similaires de suivi non désiré peuvent pénétrer dans l'équipement terminal de l'utilisateur final à son insu afin d'accéder à des informations, de stocker des informations cachées et de suivre les activités. La collecte d'informations relatives au dispositif de l'utilisateur final aux fins de l'identification et du suivi est également possible à distance, à l'aide de techniques telles que la «capture d'empreintes numériques», souvent à l'insu de l'utilisateur final, et peut porter gravement atteinte à la vie privée de celui-ci. Les techniques qui permettent de

contrôler subrepticement les actions de l'utilisateur final, par exemple en suivant ses activités en ligne ou la localisation de son équipement terminal, ou qui pervertissent le fonctionnement de l'équipement terminal de l'utilisateur final représentent une menace sérieuse pour la vie privée de celui-ci. Par conséquent, une telle interférence avec l'équipement terminal de l'utilisateur final ne devrait être autorisée qu'avec le consentement de celui-ci et à des fins précises et transparentes.

(21) Les exceptions à l'obligation d'obtenir un consentement pour utiliser les fonctions de traitement et de stockage de l'équipement terminal ou pour accéder à des informations qui y sont stockées devraient être limitées aux situations qui n'impliquent aucune intrusion, ou qu'une intrusion très limitée, dans la vie privée. Par exemple, le consentement ne devrait pas être requis pour autoriser le stockage ou l'accès techniques dès lors qu'ils sont strictement nécessaires et proportionnés à l'objectif légitime de permettre l'utilisation d'un service spécifique expressément demandé par l'utilisateur final. Cela peut comprendre le stockage de cookies, pour la durée d'une session individuelle établie sur un site Web, afin de garder une trace des données de l'utilisateur final lorsqu'il y a lieu de remplir des formulaires en ligne sur plusieurs pages. Les cookies peuvent aussi être un moyen légitime et utile de mesurer, par exemple, le trafic vers un site Web. Le fait, pour un fournisseur de services de la société de l'information, de vérifier une configuration afin de fournir un service conformément aux paramètres de l'utilisateur final, et de consigner simplement que le dispositif de celui-ci ne permet pas de recevoir le contenu demandé par l'utilisateur final ne devrait pas être considéré comme un accès audit dispositif ni comme une utilisation des fonctions de traitement du dispositif.

(22) Les méthodes utilisées pour fournir des informations et obtenir le consentement de l'utilisateur final devraient être aussi conviviales que possible. Étant donné l'usage généralisé des cookies traceurs et autres techniques de suivi, il est de plus en plus souvent demandé à l'utilisateur final de consentir au stockage de tels cookies dans son équipement terminal. En conséquence, les utilisateurs finaux sont débordés par les demandes de consentement. Le recours à des moyens techniques permettant de donner son consentement, par exemple, à l'aide de paramètres transparents et conviviaux, peut constituer une solution à ce problème. Par conséquent, le présent règlement devrait prévoir la possibilité d'exprimer un consentement en utilisant les paramètres appropriés d'un navigateur ou d'une autre application. Les choix effectués par l'utilisateur final lorsqu'il définit les paramètres généraux de confidentialité d'un navigateur ou d'une autre application devraient être contraignants pour les tiers et leur être opposables. Les navigateurs Web sont un type d'applications logicielles permettant la récupération et la présentation d'informations sur Internet. D'autres types d'applications, comme ceux qui permettent d'appeler et d'envoyer des messages ou de fournir des indications routières, ont aussi les mêmes fonctionnalités. Les navigateurs Web assurent une grande partie des interactions entre l'utilisateur final et le site Web. De ce point de vue, ils sont bien placés pour jouer un rôle actif consistant à aider l'utilisateur final à maîtriser le flux d'informations à destination et en provenance de son équipement terminal. En particulier, les navigateurs Web peuvent servir de portiers et donc aider l'utilisateur final à empêcher l'accès à des informations de son équipement terminal (smartphone, tablette ou ordinateur, par exemple) ou le stockage de telles informations.

(23) Les principes de protection des données dès la conception et de protection des données par défaut ont été consacrés par l'article 25 du règlement (UE) 2016/679. Or le

paramétrage par défaut des cookies consiste, dans la plupart des navigateurs actuels, à «accepter tous les cookies». Par conséquent, les fournisseurs de logiciels permettant la récupération et la présentation d'informations sur Internet devraient être tenus de configurer les logiciels de manière à ce qu'ils offrent la possibilité d'empêcher les tiers de stocker des informations sur les équipements terminaux. Cette option correspond souvent à la formule «rejeter les cookies de tiers». Les utilisateurs finaux devraient disposer d'un éventail de réglages de confidentialité, depuis les plus restrictifs (par exemple, «ne jamais accepter les cookies») jusqu'aux plus permissifs (par exemple, «toujours accepter les cookies»), en passant par des options intermédiaires (par exemple, «rejeter les cookies de tiers» ou «accepter uniquement les cookies propres»). Ces paramètres de confidentialité devraient se présenter sous une forme facile à visualiser et à comprendre.

(24) Pour obtenir le consentement de l'utilisateur final d'équipements terminaux au sens du règlement (UE) 2016/679, par exemple, pour le stockage de cookies traceurs de tiers, les navigateurs Web devraient notamment lui demander de manifester par un acte positif clair qu'il donne de façon libre, spécifique, éclairée et univoque son accord au stockage et à la consultation de ces cookies sur ses équipements terminaux. L'acte en question peut être considéré comme positif, par exemple, si les utilisateurs finaux sont tenus de sélectionner volontairement l'option «accepter les cookies de tiers» pour confirmer leur consentement et s'ils reçoivent les informations nécessaires pour effectuer leur choix. À cette fin, il y a lieu d'imposer aux fournisseurs de logiciels permettant d’accéder à Internet l'obligation de faire en sorte qu'au moment de l'installation, les utilisateurs finaux soient informés de la possibilité de choisir leurs paramètres de confidentialité parmi les diverses options proposées et soient invités à opérer un choix. Les informations fournies ne devraient pas dissuader les utilisateurs finaux d'opter pour une confidentialité très stricte et devraient comprendre des renseignements utiles sur les risques qu'implique le consentement au stockage de cookies de tiers sur l'ordinateur, parmi lesquels la conservation à long terme des historiques de navigation des personnes concernées et leur utilisation pour l'envoi de publicités ciblées. Les navigateurs Web sont encouragés à proposer aux utilisateurs finaux des moyens faciles de modifier leurs paramètres de confidentialité à tout moment en cours d'utilisation et à leur permettre de prévoir des exceptions ou d'établir une liste blanche de certains sites Web ou de préciser les sites Web dont ils acceptent toujours ou n'acceptent jamais les cookies (de tiers).

(25) L'accès aux réseaux de communications électroniques suppose l'envoi régulier de certains paquets de données pour rechercher ou maintenir une connexion avec le réseau ou d'autres dispositifs reliés au réseau. De plus, une adresse unique doit être assignée à chaque appareil pour qu'il soit identifiable sur ce réseau. De la même façon, les normes en matière de communications sans fil et de téléphonie cellulaire prévoient l'émission de signaux actifs contenant des identificateurs uniques tels qu’une adresse MAC, l'IMEI (numéro d'identification des équipements terminaux GSM), l'IMSI, etc. Une station de base sans fil (c'est-à-dire un transmetteur ou un récepteur) isolée, telle qu'un point d'accès sans fil, possède une portée spécifique en deçà de laquelle ces informations peuvent être captées. Des fournisseurs proposent désormais des services de suivi fondés sur le balayage des informations liées aux équipements à diverses fins, comme le comptage de personnes, la fourniture de données sur le nombre de personnes dans une file d'attente, le calcul du nombre de personnes se trouvant dans un périmètre précis, etc. Ces informations peuvent être utilisées à des fins plus intrusives, comme l'envoi de messages commerciaux à l'utilisateur final lui proposant des offres

personnalisées, par exemple, lorsqu'il entre dans un magasin. Si certaines de ces fonctionnalités ne comportent pas de risques importants pour la vie privée, d'autres peuvent y porter atteinte, comme celles qui impliquent le suivi de personnes dans le temps, y compris des visites répétées dans des lieux déterminés. Les fournisseurs qui recourent à cette pratique devraient faire apparaître de manière bien visible un message à la périphérie de la zone de couverture pour informer l'utilisateur final de l'équipement terminal, avant qu'il ne pénètre dans la zone définie, de la présence de cette technologie dans un périmètre donné, de la finalité du suivi effectué, de la personne qui en est responsable et des mesures éventuelles qu'il peut prendre pour réduire au minimum la collecte d'informations ou la faire cesser. Des informations supplémentaires devraient être fournies lorsque des données à caractère personnel sont collectées en application de l'article 13 du règlement (UE) 2016/679.

(26) Lorsque le traitement des données de communications électroniques par les fournisseurs de services de communications électroniques entrera dans son champ d'application, le présent règlement devrait prévoir la possibilité, pour l'Union ou les États membres, de légiférer afin de limiter, dans des conditions précises, certaines obligations et certains droits lorsqu'une telle limitation constitue une mesure nécessaire et proportionnée dans une société démocratique pour préserver certains intérêts publics, comme la sûreté nationale, la défense, la sécurité publique ainsi que la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, et pour garantir d'autres objectifs d'intérêt public importants de l'Union ou d'un État membre, notamment un intérêt économique ou financier important de l'Union ou d'un État membre, ou une fonction de contrôle, d'inspection ou de réglementation participant à l’exercice de l’autorité publique relativement à ces intérêts. Ainsi le présent règlement devrait-il être sans effet sur la faculté que possèdent les États membres de procéder à l'interception légale des communications électroniques ou d’arrêter d’autres mesures si cela s'avère nécessaire et proportionné pour assurer la sauvegarde des intérêts publics visés ci-dessus, conformément à la Charte des droits fondamentaux de l'Union européenne et à la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, telles qu’elles ont été interprétées par la Cour de justice de l'Union européenne et par la Cour européenne des droits de l’homme. Les fournisseurs de services de communications devraient prévoir des procédures appropriées afin de faciliter le traitement des demandes légitimes des autorités compétentes en tenant compte, le cas échéant, du rôle du représentant désigné en application de l'article 3, paragraphe 3.

(27) En ce qui concerne l'identification de la ligne appelante, il est nécessaire 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. Certains utilisateurs finaux, en particulier les services d'assistance téléphonique et les autres organismes similaires, ont intérêt à garantir l'anonymat de ceux qui les appellent. En ce qui concerne l'identification de la ligne connectée, il est nécessaire 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 d'un appel est effectivement connecté.

(28) Dans des cas spécifiques, il est justifié d'empêcher que la présentation de l'identification de la ligne appelante soit supprimée. Une limitation du droit de

l'utilisateur final à la vie privée devrait être prévue en ce qui concerne l'identification de la ligne appelante lorsque cela est nécessaire pour déterminer l'origine d'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, comme eCall, d'intervenir le plus efficacement possible.

(29) Il existe différents moyens techniques qui permettent aux fournisseurs de services de communications électroniques de limiter la réception d'appels indésirables par les utilisateurs finaux, comme le blocage des appels silencieux et autres appels frauduleux et malveillants. Les fournisseurs de services de communications interpersonnelles fondés sur la numérotation et accessibles au public devraient déployer ces moyens techniques et protéger gratuitement les utilisateurs finaux contre les appels malveillants. Les fournisseurs devraient veiller à ce que les utilisateurs finaux soient informés de l'existence de telles fonctionnalités en l'annonçant sur leur site Web.

(30) Les annuaires accessibles au public, répertoriant les utilisateurs finaux de services de communications électroniques, font l'objet d'une large diffusion. Par annuaire accessible au public il faut entendre tout annuaire ou service contenant des informations sur les utilisateurs finaux, tels que des numéros de téléphone (y compris de téléphone mobile) et des coordonnées de contact par courriel, et proposant des services de renseignement. En vertu du droit au respect de la vie privée et à la protection des données à caractère personnel des personnes physiques, il y a lieu de demander leur consentement aux utilisateurs finaux qui sont des personnes physiques avant d'enregistrer leurs données personnelles dans un annuaire. L'intérêt légitime des personnes morales exige que les utilisateurs finaux qui sont des personnes morales jouissent du droit de s'opposer à ce que des données les concernant soient enregistrées dans un annuaire.

(31) Si les utilisateurs finaux qui sont des personnes physiques consentent à l'enregistrement de leurs données dans un tel annuaire, ils devraient pouvoir déterminer, sur la base du consentement, quelles catégories de données à caractère personnel peuvent figurer dans l'annuaire (par exemple, nom, adresse électronique, adresse du domicile, nom d'utilisateur, numéro de téléphone). En outre, les fournisseurs d'annuaires accessibles au public devraient informer les utilisateurs finaux des finalités de l'annuaire et des fonctions de consultation qu'il propose avant de les y enregistrer. Les utilisateurs finaux devraient pouvoir déterminer, sur la base du consentement, les catégories de données à caractère personnel à partir desquelles leurs coordonnées peuvent être consultées. Les catégories de données à caractère personnel figurant dans l'annuaire et les catégories de données à caractère personnel à partir desquelles les coordonnées de l'utilisateur final peuvent être consultées ne devraient pas nécessairement coïncider.

(32) Dans le présent règlement, on entend par prospection directe toute forme de publicité à laquelle s'adonne une personne physique ou morale pour adresser directement des communications de prospection à un ou plusieurs utilisateurs finaux identifiés ou identifiables de services de communications électroniques. Outre l'offre de produits et de services à des fins commerciales, la notion devrait s'étendre également aux messages que les partis politiques envoient à des personnes physiques, en recourant aux services de communications électroniques, afin d'assurer leur promotion. Il devrait en être de même pour les messages envoyés par d'autres organisations à but non lucratif pour servir les objectifs de l'organisation.

(33) Des garanties devraient être prévues pour protéger l'utilisateur final contre les communications non sollicitées à des fins de prospection directe qui portent atteinte à sa vie privée. Le degré d'atteinte à la vie privée et de malveillance est jugé relativement similaire quels que soient la technique ou le canal utilisés, parmi la vaste panoplie de moyens existant, pour effectuer ces communications électroniques, qu'il s'agisse de systèmes de communication et d'appel automatisés, d'applications de messagerie instantanée, de courriels, de SMS, de MMS, de Bluetooth, etc. Il se justifie, dès lors, d'imposer que le consentement de l'utilisateur final soit obtenu avant que lui soient envoyées des communications électroniques commerciales à des fins de prospection directe, de manière à protéger efficacement les personnes contre les atteintes à leur vie privée ainsi que l'intérêt légitime des personnes morales. Dans un souci de sécurité juridique et de pérennité des règles de protection contre les communications électroniques non sollicitées, il convient d'établir un ensemble unique de règles qui ne varient pas en fonction de la technique utilisée pour l'acheminement de ces communications non sollicitées, tout en assurant un niveau de protection équivalent à tous les Européens. Il est cependant raisonnable d'autoriser l'utilisation des adresses électroniques dans le cadre d'une relation client-fournisseur existante pour proposer au client des produits ou des services similaires. Cette possibilité devrait se limiter à l'entreprise qui a obtenu les coordonnées électroniques en application du règlement (UE) 2016/679.

(34) Lorsque les utilisateurs finaux ont consenti à la réception de communications non sollicitées à des fins de prospection directe, ils devraient conserver la faculté de retirer facilement leur consentement à tout moment. Afin de faciliter la mise en œuvre effective des règles de l'Union relatives aux messages de prospection directe non sollicités, il importe d'interdire l'envoi de messages commerciaux non sollicités à des fins de prospection directe sous une fausse identité, une fausse adresse de réponse ou un faux numéro. Par conséquent, il convient que les communications de prospection non sollicitées soient clairement identifiables comme telles, qu'elles mentionnent l'identité de la personne morale ou physique qui transmet la communication ou pour le compte de laquelle la communication est transmise et qu'elles fournissent les informations nécessaires aux destinataires pour leur permettre d'exercer leur droit de refuser de continuer à recevoir des messages de prospection écrits et/ou oraux.

(35) Afin de faciliter le retrait du consentement, les personnes morales ou physiques effectuant des communications de prospection directe par courrier électronique devraient présenter un lien ou une adresse de courrier électronique valable, que les utilisateurs finaux puissent aisément utiliser pour retirer leur consentement. Les personnes morales ou physiques qui effectuent des communications de prospection directe sous la forme d'appels vocaux ou à l'aide de systèmes de communication et d'appel automatisés devraient s'identifier en affichant la ligne directe sur laquelle l'entreprise peut être appelée ou devraient présenter un code spécifique indiquant qu'il s'agit d'un appel commercial.

(36) Les appels vocaux de prospection directe effectués sans recourir à des systèmes de communication et d'appel automatisés sont plus onéreux pour l'émetteur et n'imposent pas de charge financière à l'utilisateur final. Les États membres devraient, dès lors, être en mesure de créer et/ou de maintenir des systèmes nationaux autorisant uniquement ce type d'appels à destination des utilisateurs finaux qui n'ont pas formulé d'objection.

(37) Les fournisseurs de services qui proposent des services de communications électroniques devraient informer les utilisateurs finaux des mesures qu'ils peuvent prendre pour préserver la sécurité de leurs communications en utilisant, par exemple, des types de logiciels ou des techniques de cryptage spécifiques. L'obligation qui est faite à un fournisseur de services d'informer les utilisateurs finaux 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. La sécurité s'apprécie au regard de l'article 32 du règlement (UE) 2016/679.

(38) Dans un souci de parfaite concordance avec le règlement (UE) 2016/679, le contrôle de l'application des dispositions du présent règlement devrait être confié aux mêmes autorités que celles qui sont chargées du contrôle de l'application des dispositions du règlement (UE) 2016/679, le présent règlement reposant sur le mécanisme de contrôle de la cohérence du règlement (UE) 2016/679. Les États membres devraient pouvoir disposer de plusieurs autorités de contrôle en fonction de leur structure constitutionnelle, organisationnelle et administrative. Les autorités de contrôle devraient aussi être responsables du suivi de l'application du présent règlement relativement aux données de communications électroniques concernant les personnes morales. Ces tâches supplémentaires ne devraient pas compromettre la capacité de l'autorité de contrôle de remplir ses missions de protection des données à caractère personnel en vertu du règlement (UE) 2016/679 et du présent règlement. Chaque autorité de contrôle devrait être dotée des ressources financières et humaines, des locaux et des infrastructures supplémentaires nécessaires à l'exécution effective des tâches prévues par le présent règlement.

(39) Chaque autorité de contrôle devrait être habilitée, sur le territoire de son propre État membre, à exercer les compétences et exécuter les tâches prévues par le présent règlement. Afin d'assurer la cohérence du contrôle et de l'application du présent règlement dans l'ensemble de l'Union, les autorités de contrôle devraient avoir, dans chaque État membre, les mêmes missions et les mêmes pouvoirs effectifs, sans préjudice des pouvoirs des autorités chargées des poursuites en vertu du droit d'un État membre, pour porter les violations du présent règlement à l'attention des autorités judiciaires et ester en justice. Les États membres et leurs autorités de contrôle sont encouragés à prendre en considération les besoins spécifiques des micro, petites et moyennes entreprises dans le cadre de l'application du présent règlement.

(40) Afin de renforcer le contrôle de l'application des règles du présent règlement, chaque autorité de contrôle devrait avoir le pouvoir d'infliger des sanctions, y compris des amendes administratives en cas d'infraction au présent règlement, en lieu et place ou en sus de toute autre mesure appropriée en application du présent règlement. Le présent règlement devrait définir les violations, le montant maximal et les critères de fixation des amendes administratives dont elles sont passibles, qui devraient être fixés par l'autorité de contrôle compétente dans chaque cas d'espèce, en prenant en considération toutes les caractéristiques propres à chaque cas et compte dûment tenu, notamment, de la nature, de la gravité et de la durée de la violation et de ses conséquences, ainsi que des mesures prises pour garantir le respect des obligations découlant du règlement et pour prévenir ou atténuer les conséquences de la violation. Aux fins de l'imposition d'une amende au titre du présent règlement, il faut entendre par entreprise une entreprise au sens des articles 101 et 102 du traité.

(41) Afin de remplir les objectifs du présent règlement, à savoir protéger les libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel, et garantir la libre circulation de ces données au sein de l'Union, il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément à l'article 290 du traité. Des actes délégués devraient notamment être adoptés en ce qui concerne les informations à présenter, y compris au moyen d'icônes normalisées, afin d'offrir une vue d'ensemble, facile à visualiser et à comprendre, de la collecte des informations émises par un équipement terminal, de sa finalité, de la personne qui en est responsable et des mesures éventuelles que l'utilisateur final de l'équipement terminal peut prendre pour réduire au minimum la collecte d'informations. Des actes délégués sont également nécessaires pour définir un code permettant d'identifier les appels de prospection directe, y compris les appels effectués au moyen de systèmes de communication et d'appel automatisés. Il est particulièrement important que la Commission procède à des consultations appropriées et que ces consultations soient menées conformément aux principes établis dans l'accord interinstitutionnel «Mieux légiférer» du 13 avril 2016[8]. En particulier, pour assurer leur égale participation à la préparation des actes délégués, le Parlement européen et le Conseil reçoivent tous les documents au même moment que les experts des États membres, et leurs experts ont systématiquement accès aux réunions des groupes d'experts de la Commission traitant de la préparation des actes délégués. De plus, afin d'assurer des conditions uniformes d'exécution du présent règlement, il convient de conférer des compétences d'exécution à la Commission lorsque le présent règlement le prévoit. Ces compétences devraient être exercées en conformité avec le règlement (UE) n° 182/2011.

(42) Étant donné que l'objectif du présent règlement, à savoir assurer un niveau équivalent de protection des personnes physiques et morales et la libre circulation des données de communications électroniques dans l'ensemble de l'Union, ne peut pas être atteint de manière suffisante par les États membres mais peut, en raison des dimensions ou des effets de l'action, l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures, conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité tel qu'énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre cet objectif.

(43) Il y a lieu d'abroger la directive 2002/58/CE,

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

[8] Accord interinstitutionnel entre le Parlement européen, le Conseil de l'Union européenne et la Commission européenne «Mieux légiférer» du 13 avril 2016 (JO L 123 du 12.5.2016, p. 1).

CHAPITRE I
DISPOSITIONS GÉNÉRALES

Article premier
Objet

1. Le présent règlement établit les règles relatives à la protection des libertés et droits fondamentaux des personnes physiques et morales en ce qui concerne la fourniture et l'utilisation de services de communications électroniques, et notamment le droit au respect de la vie privée et des communications et la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

2. Le présent règlement garantit la libre circulation des données de communications électroniques et des services de communications électroniques au sein de l'Union, qui n'est ni limitée ni interdite pour des motifs liés au respect de la vie privée et des communications des personnes physiques et morales et à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

3. Les dispositions du présent règlement précisent et complètent le règlement (UE) 2016/679 en établissant des règles spécifiques aux fins visées aux paragraphes 1 et 2.

Article 2
Champ d'application matériel

1. Le présent règlement s'applique au traitement des données de communications électroniques effectué en relation avec la fourniture et l'utilisation de services de communications électroniques dans l'Union et aux informations liées aux équipements terminaux des utilisateurs finaux.

2. Le présent règlement ne s'applique pas:

(a) aux activités qui ne relèvent pas du champ d'application du droit de l'Union;

(b) aux activités des États membres qui relèvent du champ d'application du titre V, chapitre 2, du traité sur l'Union européenne;

(c) aux services de communications électroniques qui ne sont pas accessibles au public;

(d) aux activités menées par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces.

3. Le traitement des données de communications électroniques par les institutions, organes et organismes de l'Union est régi par le règlement (UE) n° 00/0000 [nouveau règlement remplaçant le règlement 45/2001].

4. Le présent règlement s'applique sans préjudice de la directive 2000/31/CE[9], et notamment de ses articles 12 à 15 relatifs à la responsabilité des prestataires de services intermédiaires.

5. Le présent règlement s'applique sans préjudice des dispositions de la directive 2014/53/UE.

Article 3
Champ d'application territorial et représentant

1. Le présent règlement s'applique:

(e) à la fourniture de services de communications électroniques aux utilisateurs finaux dans l'Union, qu'un paiement soit requis ou non de la part de l'utilisateur final;

(f) à l'utilisation de ces services;

(g) à la protection des informations liées aux équipements terminaux des utilisateurs finaux situés dans l'Union.

2. Lorsque le fournisseur d'un service de communications électroniques n'est pas établi dans l'Union, il désigne par écrit un représentant dans l'Union.

3. Le représentant est établi dans l'un des États membres dans lesquels sont situés les utilisateurs finaux dudit service de communications électroniques.

4. Le représentant est habilité à répondre aux questions et à fournir des informations en sus ou à la place du fournisseur qu'il représente, notamment à l'intention des autorités de contrôle et des utilisateurs finaux, sur tout problème concernant le traitement des données de communications électroniques aux fins de garantir la conformité au présent règlement.

5. La désignation d'un représentant en vertu du paragraphe 2 est sans préjudice des poursuites qui pourraient être intentées contre une personne physique ou morale qui traite des données de communications électroniques en relation avec la fourniture de services de communications électroniques assurée depuis l'extérieur de l'Union à l'intention d'utilisateurs finaux situés dans l'Union.

Article 4
Définitions

1. Aux fins du présent règlement, les définitions suivantes s'appliquent:

[9] 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») (JO L 178 du 17.7.2000, p. 1).

(h) les définitions du règlement (UE) 2016/679;

(i) les définitions de «réseau de communications électroniques», «service de communications électroniques», «service de communications interpersonnelles», «service de communications interpersonnelles fondé sur la numérotation», «service de communications interpersonnelles non fondé sur la numérotation», «utilisateur final» et «appel» figurant respectivement à l'article 2, points 1), 4), 5), 6), 7), 14) et 21) de la [directive établissant le code des communications électroniques européen];

(j) la définition d'«équipement terminal» figurant à l'article 1er, point 1), de la directive 2008/63/CE de la Commission[10].

2. Aux fins du paragraphe 1, point b), la définition de «service de communications interpersonnelles» comprend les services qui rendent possible une communication interpersonnelle et interactive uniquement en tant que fonction mineure accessoire intrinsèquement liée à un autre service.

3. En outre, aux fins du présent règlement, on entend par:

(k) «données de communications électroniques» le contenu de communications électroniques et les métadonnées de communications électroniques;

(l) «contenu de communications électroniques» le contenu échangé au moyen de services de communications électroniques, notamment sous forme de texte, de voix, de documents vidéo, d'images et de son;

(m) «métadonnées de communications électroniques» les données traitées dans un réseau de communications électroniques aux fins de la transmission, la distribution ou l'échange de contenu de communications électroniques, y compris les données permettant de retracer une communication et d'en déterminer l'origine et la destination ainsi que les données relatives à la localisation de l'appareil produites dans le cadre de la fourniture de services de communications électroniques, et la date, l'heure, la durée et le type de communication;

(n) «annuaire accessible au public» un annuaire des utilisateurs finaux de services de communications électroniques, sur support imprimé ou électronique, qui est publié ou mis à la disposition du public ou d'une partie du public, y compris par l'intermédiaire d'un service de renseignements;

(o) «courrier électronique» tout message électronique contenant des informations 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, dans des installations informatiques connexes ou dans l'équipement terminal de son destinataire;

(p) «communications de prospection directe» toute forme de publicité, tant écrite qu'orale, envoyée à un ou plusieurs utilisateurs finaux, identifiés ou identifiables, de services de communications électroniques, y compris au moyen de systèmes de

[10] Directive 2008/63/CE de la Commission du 20 juin 2008 relative à la concurrence dans les marchés des équipements terminaux de télécommunications (JO L 162 du 21.6.2008, p. 20).

communication et d'appel automatisés, avec ou sans intervention humaine, par courrier électronique, par SMS, etc.;

(q) «appels vocaux de prospection directe» les appels effectués en direct sans recourir à des systèmes de communication et d'appel automatisés;

(r) «systèmes de communication et d'appel automatisés» les systèmes capables de passer des appels de manière automatique à un ou plusieurs destinataires conformément aux instructions établies pour ce système et de transmettre des sons ne consistant pas en une conversation de vive voix, notamment des appels effectués à l'aide de systèmes de communication et d'appel automatisés qui relient la personne appelée à une personne physique.

CHAPITRE II
PROTECTION DES COMMUNICATIONS ÉLECTRONIQUES DES PERSONNES PHYSIQUES ET MORALES ET DES INFORMATIONS STOCKÉES DANS LEURS ÉQUIPEMENTS TERMINAUX

Article 5
Confidentialité des données de communications électroniques

Les données de communications électroniques sont confidentielles. Toute interférence avec des données de communications électroniques, comme l'écoute, l'enregistrement, le stockage, la surveillance et d'autres types d'interception, de surveillance ou de traitement des données de communications électroniques, par des personnes autres que l'utilisateur final est interdite, sauf dans les cas où le présent règlement l'autorise.

Article 6
Traitement autorisé des données de communications électroniques

1. Les fournisseurs de réseaux et de services de communications électroniques peuvent traiter les données de communications électroniques si:

(s) cela est nécessaire pour assurer la communication, pendant la durée nécessaire à cette fin; ou

(t) cela est nécessaire pour maintenir ou rétablir la sécurité des réseaux et services de communications électroniques ou détecter des défaillances techniques et/ou des erreurs dans la transmission des communications électroniques, pendant la durée nécessaire à cette fin.

2. Les fournisseurs de services de communications électroniques peuvent traiter les métadonnées de communications électroniques si:

(u) cela est nécessaire pour satisfaire aux prescriptions obligatoires en matière de qualité de service prévues par la [directive établissant le code des communications

électroniques européen] ou le règlement (UE) 2015/2120[11], pendant la durée nécessaire à cette fin; ou

(v) cela est nécessaire pour établir les factures, calculer les paiements pour interconnexion, détecter ou faire cesser les fraudes à l'usage et à l'abonnement en matière de services de communications électroniques; ou

(w) l'utilisateur final concerné a donné son consentement au traitement de ses métadonnées de communications pour un ou plusieurs objectifs précis, dont la fourniture de services spécifiques à son endroit, à condition que le traitement d'informations anonymisées ne permette pas d'atteindre lesdits objectifs.

3. Les fournisseurs des services de communications électroniques peuvent traiter le contenu de communications électroniques uniquement:

(x) afin de fournir un service spécifique à un utilisateur final, si l'utilisateur ou les utilisateurs finaux concernés ont donné leur consentement au traitement de leur contenu de communications électroniques et si la fourniture du service ne peut être assurée sans traiter ce contenu; ou

b) si tous les utilisateurs finaux concernés ont donné leur consentement au traitement de leur contenu de communications électroniques pour un ou plusieurs objectifs spécifiques que le traitement d'informations anonymisées ne permet pas d'atteindre et si le fournisseur a consulté l'autorité de contrôle. Les points 2) et 3) de l'article 36 du règlement (UE) 2016/679 s'appliquent à la consultation de l'autorité de contrôle.

Article 7
Stockage et effacement des données de communications électroniques

1. Sans préjudice de l'article 6, paragraphe 1, point b), et de l'article 6, paragraphe 3, points a) et b), le fournisseur de services de communications électroniques efface le contenu de communications électroniques ou anonymise les données après réception du contenu de communications électroniques par le ou les destinataires. Ces données peuvent être enregistrées ou stockées par les utilisateurs finaux ou un tiers mandaté par eux pour assurer l'enregistrement, le stockage ou tout autre traitement de ces données, conformément aux dispositions du règlement (UE) 2016/679.

2. Sans préjudice de l'article 6, paragraphe 1, point b), et de l'article 6, paragraphe 2, points a) et c), le fournisseur de services de communications électroniques efface les métadonnées de communications électroniques ou anonymise les données lorsqu'elles ne sont plus nécessaires pour assurer la communication.

3. Lorsque le traitement des métadonnées de communications s'effectue à des fins de facturation conformément à l'article 6, paragraphe 2, point b), les métadonnées en question peuvent être conservées jusqu'à la fin de la période au cours de laquelle la

[11] Règlement (UE) 2015/2120 du Parlement européen et du Conseil du 25 novembre 2015 établissant des mesures relatives à l'accès à un internet ouvert et modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques et le règlement (UE) n° 531/2012 concernant l'itinérance sur les réseaux publics de communications mobiles à l'intérieur de l'Union, JO L 310 du 26.11.2015, p. 1.

facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement en application du droit national.

Article 8
Protection des informations stockées dans les équipements terminaux des utilisateurs finaux ou liées à ces équipements

1. L'utilisation des capacités de traitement et de stockage des équipements terminaux et la collecte d'informations provenant des équipements terminaux des utilisateurs finaux, y compris sur les logiciels et le matériel, sont interdites, sinon par l'utilisateur final concerné et pour les motifs suivants:

(y) si cela est nécessaire à la seule fin d'assurer une communication électronique dans un réseau de communications électroniques; ou

(z) si l'utilisateur final a donné son consentement; ou

(aa) si cela est nécessaire pour fournir un service de la société de l'information demandé par l'utilisateur final; ou

(bb) si cela est nécessaire pour mesurer des résultats d'audience sur le Web, à condition que ce mesurage soit effectué par le fournisseur du service de la société de l'information demandé par l'utilisateur final.

2. La collecte d'informations émises par l'équipement terminal pour permettre sa connexion à un autre dispositif ou à un équipement de réseau est interdite, sauf si:

(cc) elle est pratiquée exclusivement dans le but d'établir une connexion et pendant la durée nécessaire à cette fin; ou

(dd) un message clair et bien visible est affiché, indiquant les modalités et la finalité de la collecte et la personne qui en est responsable, fournissant les autres informations requises en vertu de l'article 13 du règlement (UE) 2016/679 lorsque la collecte porte sur des données à caractère personnel, et précisant les mesures éventuelles que peut prendre l'utilisateur final de l'équipement terminal pour réduire au minimum la collecte ou la faire cesser.

La collecte de ces informations est subordonnée à la mise en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, comme le prévoit l'article 32 du règlement (UE) 2016/679.

3. Les informations à fournir en application du paragraphe 2, point b), peuvent être associées à des icônes normalisées de manière à offrir une vue d'ensemble efficace de la collecte, qui soit facile à visualiser, à comprendre et à lire.

4. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 27 déterminant les informations à présenter au moyen de l'icône normalisée ainsi que les procédures régissant la fourniture d'icônes normalisées.

Article 9
Consentement

1. La définition et les conditions du consentement figurant à l'article 4, paragraphe 11, et à l'article 7 du règlement (UE) 2016/679/UE s'appliquent.

2. Sans préjudice du paragraphe 1, si cela est techniquement possible et réalisable, aux fins de l'article 8, paragraphe 1, le consentement peut être exprimé à l'aide des paramètres techniques appropriés d'une application logicielle permettant d'accéder à Internet.

3. Les utilisateurs finaux qui ont donné leur consentement au traitement de données de communications électroniques conformément à l'article 6, paragraphe 2, point c), et à l'article 6, paragraphe 3, points a) et b), ont la possibilité de retirer leur consentement à tout moment, comme prévu à l'article 7, paragraphe 3, du règlement (UE) 2016/679, et cette possibilité leur est rappelée tous les six mois tant que le traitement se poursuit.

Article 10
Informations à fournir et options à proposer pour les paramètres de confidentialité

1. Les logiciels mis sur le marché qui permettent d'effectuer des communications électroniques, y compris la récupération et la présentation d'informations sur Internet, offrent la possibilité d'empêcher les tiers de stocker des informations sur l'équipement terminal d'un utilisateur final ou de traiter des informations déjà stockées sur ledit terminal.

2. Au moment de l'installation, le logiciel informe l'utilisateur final des paramètres de confidentialité disponibles et, avant de continuer l'installation, lui impose d'en accepter un.

3. Dans le cas d'un logiciel qui était déjà installé à la date du 25 mai 2018, les exigences visées aux paragraphes 1 et 2 sont remplies au moment de la première mise à jour du logiciel, mais au plus tard le 25 août 2018.

Article 11
Limitations

1. Le droit de l'Union ou le droit des États membres peuvent, par la voie de mesures législatives, limiter la portée des obligations et des droits prévus aux articles 5 à 8 lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire, appropriée et proportionnée dans une société démocratique pour préserver un ou plusieurs des intérêts publics visés à l'article 23, paragraphe 1, points a) à e), du règlement (UE) 2016/679 ou une fonction de contrôle, d'inspection ou de réglementation participant à l'exercice de l'autorité publique relativement à ces intérêts.

2. Les fournisseurs de services de communications électroniques établissent des procédures internes permettant de répondre aux demandes d'accès aux données de communications électroniques des utilisateurs finaux formulées sur la base d'une

mesure législative adoptée au titre du paragraphe 1. Ils mettent, sur demande, à la disposition de l'autorité de contrôle compétente des informations sur ces procédures, sur le nombre de demandes reçues, sur le motif juridique invoqué et sur leur réponse.

CHAPITRE III
DROIT DE REGARD DES PERSONNES PHYSIQUES ET MORALES SUR LES COMMUNICATIONS ÉLECTRONIQUES

Article 12
Présentation et restriction de l'identification des lignes appelante et connectée

1. Dans les cas où la présentation de l'identification des lignes appelante et connectée est proposée conformément à l'article [107] de la [directive établissant le code des communications électroniques européen], les fournisseurs de services de communications interpersonnelles fondés sur la numérotation et accessibles au public offrent:

(ee) à l'utilisateur final auteur de l'appel la possibilité d'empêcher la présentation de l'identification de la ligne appelante lors de chaque appel, lors de chaque connexion ou à titre permanent;

(ff) à l'utilisateur final destinataire de l'appel la possibilité d'empêcher la présentation de l'identification de la ligne appelante pour les appels entrants;

(gg) à l'utilisateur final destinataire de l'appel la possibilité de refuser les appels entrants lorsque l'utilisateur final auteur de l'appel a empêché la présentation de l'identification de la ligne appelante;

(hh) à l'utilisateur final destinataire de l'appel la possibilité d'empêcher la présentation de l'identification de la ligne connectée à l'utilisateur final auteur de l'appel.

2. Les utilisateurs finaux jouissent des possibilités visées au paragraphe 1, points a), b), c) et d), par des moyens simples et sans frais.

3. Le paragraphe 1, point a), s'applique également aux appels provenant de l'Union à destination de pays tiers. Le paragraphe 1, points b), c) et d), s'appliquent également aux appels entrants provenant de pays tiers.

4. Dans les cas où la présentation de l'identification des lignes appelante et connectée est proposée, les fournisseurs de services de communications interpersonnelles fondés sur la numérotation et accessibles au public fournissent des informations au public sur les possibilités énoncées au paragraphe 1, points a), b), c) et d).

Article 13
Exceptions à la présentation et à la restriction de l'identification des lignes appelante et connectée

1. Dans le cas d'un appel adressé à des services d'urgence, même si l'utilisateur final auteur de l'appel a empêché la présentation de l'identification de la ligne appelante, les fournisseurs de services de communications interpersonnelles fondés sur la numérotation et accessibles au public passent outre à la suppression de la présentation de l'identification de la ligne appelante et à l'interdiction ou à l'absence de consentement d'un utilisateur final quant au traitement des métadonnées, ligne par ligne, pour les organismes chargés de traiter les communications d'urgence, y compris les centres de réception des appels d'urgence, dans le but de permettre une réaction à ces communications.

2. Les États membres arrêtent des dispositions plus précises quant à l'établissement des procédures selon lesquelles les fournisseurs de services de communications interpersonnelles fondés sur la numérotation et accessibles au public passent outre, et dans quelles circonstances, à la suppression de la présentation de l'identification de la ligne appelante à titre temporaire, lorsque des utilisateurs finaux demandent l'identification d'appels malveillants ou dérangeants.

Article 14
Blocage des appels entrants

Les fournisseurs de services de communications interpersonnelles fondés sur la numérotation et accessibles au public déploient les techniques les plus avancées pour limiter la réception d'appels indésirables par les utilisateurs finaux et offrent également, sans frais, à l'utilisateur final destinataire de l'appel les possibilités suivantes:

(ii) bloquer les appels entrants provenant de numéros précis ou de sources anonymes;

(jj) mettre fin au renvoi automatique des appels par un tiers vers l'équipement terminal de l'utilisateur final.

Article 15
Annuaires accessibles au public

1. Les fournisseurs d'annuaires accessibles au public sont tenus d'obtenir le consentement des utilisateurs finaux qui sont des personnes physiques pour enregistrer dans un annuaire les données à caractère personnel de ces utilisateurs finaux et, partant, d'obtenir leur consentement pour l'enregistrement des données par catégorie de données à caractère personnel, dans la mesure où ces données sont pertinentes pour la destination de l'annuaire telle qu'elle a été établie par son fournisseur. Les fournisseurs offrent aux utilisateurs finaux qui sont des personnes physiques les moyens de vérifier, de corriger et de supprimer ces données.

2. Les fournisseurs d'annuaires accessibles au public informent les utilisateurs finaux qui sont des personnes physiques et dont les données à caractère personnel figurent dans l'annuaire en les avisant des fonctions de recherche disponibles dans l'annuaire

et sont tenus d'obtenir le consentement des utilisateurs finaux avant d'activer ces fonctions de recherche en relation avec leurs données personnelles.

3. Les fournisseurs d'annuaires accessibles au public offrent aux utilisateurs finaux qui sont des personnes morales la possibilité de s'opposer à ce que des données les concernant soient enregistrées dans l'annuaire. Les fournisseurs offrent aux utilisateurs finaux qui sont des personnes morales les moyens de vérifier, de corriger et de supprimer ces données.

4. La possibilité, pour les utilisateurs finaux de ne pas figurer dans un annuaire accessible au public ou de vérifier, de corriger et de supprimer toutes les données les concernant, leur est offerte sans frais.

Article 16
Communications non sollicitées

1. Les personnes physiques ou morales peuvent utiliser les services de communications électroniques pour l'envoi de communications de prospection directe aux utilisateurs finaux qui sont des personnes physiques ayant donné leur consentement.

2. Lorsque, dans le respect du règlement (UE) 2016/679, une personne physique ou morale a, dans le cadre de la vente d'un produit ou d'un service, obtenu de son client ses coordonnées électroniques, 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 uniquement si le client se voit donner clairement et expressément la faculté de s'opposer, sans frais et de manière simple, à une telle exploitation. Le droit d'opposition est donné au moment où les coordonnées sont recueillies et lors de l'envoi de chaque message.

3. Sans préjudice des paragraphes 1 et 2, les personnes physiques ou morales faisant usage de services de communications électroniques pour effectuer des appels de prospection directe:

(kk) présentent l'identité d'une ligne sur laquelle elles peuvent être contactées; ou

(ll) présentent un code ou un indicatif spécifique indiquant qu'il s'agit d'un appel commercial.

4. Sans préjudice du paragraphe 1, les États membres peuvent prévoir, par des mesures législatives, que les appels vocaux de prospection directe adressés à des utilisateurs finaux qui sont des personnes physiques ne sont autorisés que si ces derniers n'ont pas exprimé d'objection à recevoir ces communications.

5. Les États membres veillent à ce que, dans le cadre du droit de l'Union et du droit national applicable, l'intérêt légitime des utilisateurs finaux qui sont des personnes morales soit suffisamment protégé à l'égard des communications non sollicitées envoyées par les moyens énoncés au paragraphe 1.

6. Toute personne physique ou morale utilisant des services de communications électroniques pour transmettre des communications de prospection directe informe les utilisateurs finaux de la nature commerciale de la communication et de l'identité

de la personne morale ou physique pour le compte de laquelle la communication est transmise, et fournit les informations nécessaires aux destinataires pour leur permettre d'exercer leur droit de retirer, de manière simple, leur consentement à continuer de recevoir des communications de prospection.

7. La Commission est habilitée à adopter des mesures d'exécution conformément à l'article 26, paragraphe 2, en vue de déterminer le code/l'indicatif à utiliser pour identifier les appels effectués à des fins de prospection en application du paragraphe 3, point b).

Article 17
Informations sur les risques de sécurité détectés

Lorsqu'il existe un risque particulier susceptible de compromettre la sécurité des réseaux et des services de communications, le fournisseur d'un service de communications électroniques en informe les utilisateurs finaux et, si les mesures que peut prendre le fournisseur du service ne permettent pas d'écarter ce risque, les informe de tout moyen éventuel d'y remédier, y compris en en indiquant le coût probable.

CHAPITRE IV
AUTORITÉS DE CONTRÔLE INDÉPENDANTES ET CONTRÔLE DE L'APPLICATION

Article 18
Autorités de contrôle indépendantes

1. L'autorité ou les autorités de contrôle indépendantes chargées du contrôle de l'application du règlement (UE) 2016/679 sont également chargées du contrôle de l'application du présent règlement. Les chapitres VI et VII du règlement (UE) 2016/679 s’appliquent par analogie. Les tâches et les compétences des autorités de contrôle sont exercées à l'égard des utilisateurs finaux.

2. L'autorité ou les autorités de contrôle visées au paragraphe 1 coopèrent, en tant que de besoin, avec les autorités de régulation nationales instituées en vertu de la [directive établissant le code des communications électroniques européen].

Article 19
Comité européen de la protection des données

Le comité européen de la protection des données institué en vertu de l'article 68 du règlement (UE) 2016/679 est compétent pour veiller à l’application cohérente du présent règlement. À cette fin, le comité européen de la protection des données s'acquitte des missions prévues à l’article 70 du règlement (UE) 2016/679. Le comité est chargé des missions suivantes:

(mm) conseiller la Commission sur tout projet de modification du présent règlement;

(nn) examiner, de sa propre initiative, à la demande de l'un de ses membres ou à la demande de la Commission, toute question portant sur l'application du présent règlement, et publier des lignes directrices, des recommandations et des bonnes pratiques afin de favoriser l'application cohérente du présent règlement;

Article 20
Procédures en matière de coopération et de cohérence

Chaque autorité de contrôle contribue à l'application cohérente du présent règlement dans l'ensemble de l'Union. À cette fin, les autorités de contrôle coopèrent entre elles et avec la Commission conformément au chapitre VII du règlement (UE) 2016/679 dans les matières couvertes par le présent règlement.

CHAPITRE V
VOIES DE RECOURS, RESPONSABILITÉ ET SANCTIONS

Article 21
Voies de recours

1. Sans préjudice de tout autre recours administratif ou juridictionnel, tout utilisateur final de services de communications électroniques dispose des mêmes voies de recours que celles prévues aux articles 77, 78 et 79 du règlement (UE) 2016/679.

2. Toute personne physique ou morale autre qu'un utilisateur final lésé par des violations du présent règlement et ayant un intérêt légitime à voir cesser ou interdire les violations présumées, y compris un fournisseur de services de communications électroniques protégeant ses intérêts commerciaux légitimes, a le droit d'agir en justice contre ces violations.

Article 22
Droit à réparation et responsabilité

Tout utilisateur final de services de communications électroniques ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir de l'auteur de la violation réparation du préjudice subi, sauf si l'auteur prouve que le fait qui a provoqué le dommage ne lui est pas imputable, conformément à l’article 82 du règlement (UE) 2016/679.

Article 23
Conditions générales pour imposer des amendes administratives

1. Aux fins du présent article, le chapitre VII du règlement (UE) 2016/679 s'applique aux violations du présent règlement.

2. Les violations des dispositions suivantes du présent règlement font l'objet, conformément au paragraphe 1, d'amendes administratives pouvant s'élever jusqu'à

10 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial de l'exercice précédent, le montant le plus élevé étant retenu:

(oo) les obligations incombant à toute personne morale ou physique qui traite des données de communications électroniques en application de l'article 8;

(pp) les obligations du fournisseur de logiciels permettant d'effectuer des communications électroniques en application de l'article 10;

(qq) les obligations du fournisseur d'annuaires accessibles au public en application de l'article 15;

(rr) les obligations incombant à toute personne morale ou physique utilisant des services de communications électroniques en application de l'article 16;

3. Les violations du principe de confidentialité des communications, du traitement autorisé des données de communications électroniques et des délais d'effacement en application des articles 5, 6 et 7 font l'objet, conformément au paragraphe 1 du présent article, d'amendes administratives pouvant s'élever jusqu'à 20 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial de l'exercice précédent, le montant le plus élevé étant retenu.

4. Les États membres déterminent le régime des sanctions applicables aux violations des articles 12, 13, 14 et 17.

5. Le non-respect d'une injonction émise par une autorité de contrôle en vertu de l'article 18 fait l'objet d'amendes administratives pouvant s'élever jusqu'à 20 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial de l'exercice précédent, le montant le plus élevé étant retenu.

6. Sans préjudice des pouvoirs dont les autorités de contrôle disposent en matière d'adoption de mesures correctrices en vertu de l'article 18, chaque État membre peut établir des règles déterminant si et dans quelle mesure des amendes administratives peuvent être imposées à des autorités publiques et à des organismes publics établis sur son territoire.

7. L'exercice, par l'autorité de contrôle, des pouvoirs que lui confère le présent article est soumis à des garanties procédurales appropriées conformément au droit de l'Union et au droit des États membres, y compris un recours juridictionnel effectif et une procédure régulière.

8. Si le système juridique d'un État membre ne prévoit pas d'amendes administratives, il est possible d'appliquer le présent article de sorte que l'amende soit déterminée par l'autorité de contrôle compétente et imposée par les juridictions nationales compétentes, en veillant à ce que ces voies de droit soient effectives et aient un effet équivalent aux amendes administratives imposées par les autorités de contrôle. En tout état de cause, les amendes imposées sont effectives, proportionnées et dissuasives. Les États membres concernés notifient à la Commission les dispositions légales qu'ils adoptent en vertu du présent paragraphe au plus tard le [xxx] et, sans tarder, toute disposition légale modificative ou modification ultérieure les concernant.

Article 24
Sanctions

1. Les États membres déterminent le régime des autres sanctions applicables en cas de violations du présent règlement, en particulier pour les violations qui ne font pas l'objet des amendes administratives prévues à l'article 23, et prennent toutes les mesures nécessaires pour garantir leur mise en œuvre. Ces sanctions sont effectives, proportionnées et dissuasives.

2. Chaque État membre notifie à la Commission les dispositions de la législation qu'il adopte en vertu du paragraphe 1, au plus tard 18 mois après la date figurant à l'article 29, paragraphe 2, et, sans délai, toute modification ultérieure l'affectant.

CHAPITRE VI
ACTES DÉLÉGUÉS ET ACTES D'EXÉCUTION

Article 25
Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.

2. Le pouvoir d'adopter les actes délégués visés à l'article 8, paragraphe 4, est conféré à la Commission pour une durée indéterminée à compter [de la date d'entrée en vigueur du présent règlement].

3. La délégation de pouvoir visée à l'article 8, paragraphe 4, peut être révoquée à tout moment par le Parlement européen ou par le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au Journal officiel de l'Union européenne ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.

4. Avant d'adopter un acte délégué, la Commission consulte les experts désignés par chaque État membre, conformément aux principes définis dans l'accord interinstitutionnel «Mieux légiférer» du 13 avril 2016.

5. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie au Parlement européen et au Conseil simultanément.

6. Un acte délégué adopté en vertu de l'article 8, paragraphe 4, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objection dans un délai de deux mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objection. Ce délai est prolongé de deux mois à l'initiative du Parlement européen ou du Conseil.

Article 26
Comité

1. La Commission est assistée par le comité des communications institué par l'article 110 de la [directive établissant le code des communications électroniques européen]. Ledit comité est un comité au sens du règlement (UE) n° 182/2011[12].

2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) n° 182/2011 s'applique.

CHAPITRE VII
DISPOSITIONS FINALES

Article 27
Abrogation

1. La directive 2002/58/CE est abrogée avec effet au 25 mai 2018.

2. Les références faites à la directive abrogée s'entendent comme faites au présent règlement.

Article 28
Suivi et évaluation

Au plus tard le 1er janvier 2018, la Commission établit un programme détaillé pour contrôler l'efficacité du présent règlement.

Au plus tard trois ans après la date de mise en application du présent règlement, et tous les trois ans par la suite, la Commission procède à une évaluation du présent règlement et présente ses principales conclusions au Parlement européen, au Conseil et au Comité économique et social européen. L'évaluation sert de base, le cas échéant, à une proposition de modification ou d'abrogation du présent règlement au vu de l'évolution de la situation juridique, technique ou économique.

Article 29
Entrée en vigueur et mise en application

1. Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

2. Il est applicable à partir du 25 mai 2018.

[12] Règlement (UE) n° 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le

Par le Parlement européen	*Par le Conseil*
Le président	*Le président*