GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

17/FR

WP 247

Avis 01/2017 sur la proposition de règlement relatif au respect de la vie privée dans les communications électroniques (2002/58/CE)

Adopté le 4 avril 2017

LE GROUPE DE PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

institué en vertu de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995,

vu les articles 29 et 30 de ladite directive,

vu son règlement intérieur,

A ADOPTÉ LE PRÉSENT AVIS:

RÉSUMÉ

Le groupe de travail salue la proposition de règlement relatif au respect de la vie privée dans les communications électroniques présentée par la Commission européenne le 10 janvier 2017. Il se félicite que le **choix se soit porté sur un règlement** comme instrument réglementaire. Un règlement garantit en effet l'uniformité des règles dans toute l'Union européenne (UE) et apporte de la clarté aux autorités de contrôle, ainsi qu'aux organisations. Il permet en outre d'assurer la cohérence avec le règlement général sur la protection des données (RGPD). Cette cohérence est en outre appuyée par le choix de confier **à l'autorité chargée de surveiller le respect du RGPD** la responsabilité du contrôle de l'application des règles relatives au respect de la vie privée dans les communications électroniques.

En même temps, le choix (maintien) d'un **instrument juridique complémentaire** est positif. La protection des communications confidentielles et de l'équipement terminal présente des caractéristiques particulières qui ne sont pas couvertes par le RGPD. Des dispositions complémentaires concernant ce type de services s'imposent donc pour garantir une protection adéquate du droit fondamental à la vie privée et à la confidentialité des communications, y compris la confidentialité de l'équipement terminal. À cet égard, le groupe de travail soutient fermement l'**approche de principe** retenue par le règlement proposé, consistant à **prévoir des interdictions très vastes et des exceptions limitées** et à **appliquer la notion de consentement de manière ciblée**.

Le groupe de travail se félicite de l'extension du champ d'application du règlement proposé pour y **inclure les opérateurs offrant des services de communication par contournement («over-the-top», OTT)**; il s'agit de services qui présentent des fonctions équivalentes aux moyens de communication plus traditionnels et peuvent donc avoir un effet similaire sur le respect de la vie privée et le droit à la confidentialité des communications des citoyens de l'UE. Il est également positif que le règlement proposé couvre clairement le **contenu et les métadonnées associées** et reconnaisse que les **métadonnées peuvent révéler des informations très sensibles.**

Le groupe de travail relève néanmoins quatre sources de **préoccupation majeure.** En ce qui concerne le **suivi de la localisation de l'équipement terminal**, **les conditions dans lesquelles l'analyse du contenu et des métadonnées est autorisée, les paramètres par défaut de l'équipement terminal et des logiciels et l'accès subordonné à l'acceptation du suivi (*tracking walls*)**, le règlement proposé abaisserait le niveau de protection octroyé par le RGPD. Dans le présent avis, le groupe de travail formule des suggestions spécifiques pour veiller à ce que le règlement relatif à la vie privée et aux communications électroniques garantisse le même niveau de protection, ou un niveau plus élevé, en adéquation avec le caractère sensible des données de communications (tant pour le contenu que pour les métadonnées).

En ce qui concerne le **suivi par Wi-Fi**, dans le cadre du RGPD, celui-ci est susceptible, en fonction des circonstances et des finalités de la collecte de données, soit d'être soumis à consentement, soit de ne pouvoir être effectué que si les données à caractère personnel sont anonymisées. Dans ce dernier cas, les quatre conditions ci-après doivent être respectées: la finalité de la collecte de données provenant de l'équipement terminal doit

se limiter à un simple comptage statistique, le suivi doit être limité dans l'espace et dans le temps à ce qui est strictement nécessaire à la réalisation de cette finalité, les données doivent être supprimées ou anonymisées immédiatement après le traitement et il doit exister des possibilités effectives de refuser cette collecte. La Commission européenne est invitée à promouvoir une norme technique permettant aux dispositifs mobiles de notifier automatiquement une objection à ce type de suivi.

En ce qui concerne l'**analyse du contenu et des métadonnées**, le point de départ devrait être l'interdiction de traiter les données de communications sans le consentement de tous les utilisateurs finaux (émetteurs et destinataires). Pour permettre aux fournisseurs d'offrir des services explicitement demandés par l'utilisateur, comme une fonction de recherche et d'indexation ou des services de synthèse vocale, il convient de prévoir une exception domestique pour le traitement du contenu et des métadonnées aux fins purement personnelles de l'utilisateur lui-même.

En ce qui concerne le **consentement au suivi**, le groupe de travail appelle à une interdiction explicite des *tracking walls*, c'est-à-dire les choix «à prendre ou à laisser» qui obligent l'utilisateur à consentir au suivi s'il souhaite accéder au service.

Dernier point, et non le moindre, le groupe de travail recommande que les équipements terminaux et les logiciels soient, **par défaut, paramétrés pour assurer la protection de la vie privée** et offrent aux utilisateurs des options claires permettant de confirmer ou de modifier ces paramètres par défaut au cours de l'installation. Ces paramètres doivent être facilement accessibles au cours de l'utilisation. L'utilisateur doit avoir la possibilité de notifier un consentement spécifique par l'intermédiaire des paramètres de son navigateur. Les préférences en matière de protection de la vie privée ne devraient pas se limiter aux interférences par des tiers ou à la question des cookies. Le groupe de travail recommande fortement de rendre obligatoire l'adhésion à la norme *Do Not Track* (interdire le suivi).

Le groupe de travail a également recensé d'autres points de préoccupation, liés par exemple au champ d'application, à la protection des équipements terminaux et à la prospection directe. Enfin, le groupe de travail a relevé certaines questions qui méritent des éclaircissements, afin de mieux protéger les utilisateurs finaux et d'assurer davantage de sécurité juridique pour tous les acteurs concernés.

SOMMAIRE

TOC

1. INTRODUCTION

1. Le groupe de travail «Article 29» sur la protection des données (ci-après le «groupe de travail» ou le «GT29») salue la proposition de la Commission européenne concernant le **règlement relatif au respect de la vie privée dans les communications électroniques** (ci-après le «règlement proposé», la «proposition de règlement» ou le «règlement relatif à la vie privée et aux communications électroniques»)[1], qui est appelé à remplacer la directive vie privée et communications électroniques[2].

2. Un grand nombre d'aspects du règlement proposé sont positifs, et la Commission européenne a effectué un grand pas en avant avec la présentation de cette proposition de règlement. Le règlement proposé peut toutefois être amélioré. Ces améliorations permettraient non seulement d'assurer une meilleure protection des utilisateurs finaux, mais également d'offrir davantage de sécurité juridique à tous les acteurs concernés.

3. Le groupe de travail nourrit ainsi des préoccupations sur plusieurs points et a formulé des recommandations de précisions à étudier par le Parlement européen et le Conseil des ministres dans le cadre de leurs débats sur la proposition de règlement. Après avoir examiné les aspects positifs du règlement proposé, le présent avis exposera les points qui sont source de préoccupation et ceux qui nécessitent des précisions.

2. POINTS POSITIFS DU RÈGLEMENT PROPOSÉ

HARMONISATION A L'ECHELLE DE L'UE, ALIGNEMENT DES AMENDES ET CONTROLE EXCLUSIF DE L'APPLICATION PAR LES AUTORITES CHARGEES DE LA PROTECTION DES DONNEES (APD)

4. Le groupe de travail se félicite que le **choix se soit porté sur un règlement comme instrument réglementaire**. Un règlement garantit l'uniformité des règles dans toute l'UE (avec certaines exceptions, qui seront examinées ci-après). Il apporte de la clarté aux autorités de contrôle, ainsi qu'aux organisations. Par ailleurs, étant donné le rôle clé que le règlement général sur la protection des données (RGPD)[3] joue dans le

[1] 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»), 2017/0003 (COD), url: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241.

[2] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), JO L 201 du 31.7.2002, p. 37, url: http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:32002L0058.

[3] 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, url: http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679.

règlement proposé, cela permet d'assurer la cohérence entre les deux instruments. En même temps, **le choix (maintien) d'un instrument juridique complémentaire** est positif. La protection des communications confidentielles et de l'équipement terminal présente des caractéristiques particulières qui ne sont pas couvertes par le RGPD. Des dispositions complémentaires concernant ce type de services s'imposent donc pour garantir une protection adéquate de ce droit fondamental. Dans ce contexte, le groupe de travail soutient également **l'approche de principe retenue par le règlement proposé, consistant à prévoir des interdictions très vastes et des exceptions limitées** et estime qu'il faut éviter l'instauration d'exceptions ouvertes sur le modèle de l'article 6 du RGPD et, en particulier, de l'article 6, point f), du RGPD (raison d'intérêts légitimes).

5. Le **contrôle de l'application de ces règles par la même autorité que celle chargée du contrôle de l'application du RGPD** permettra d'assurer une cohérence encore plus grande entre les deux instruments. Compte tenu de la relation entre la protection des données à caractère personnel et la protection des communications confidentielles et de l'équipement terminal, il est utile que le contrôle de l'application des dispositions au titre du règlement proposé soit confié à la même autorité de contrôle que celle qui est chargée du contrôle de l'application du RGPD (considérant 38 et article 18 du règlement proposé). La jurisprudence de la Cour de justice de l'Union européenne (CJUE)[4] confirme par ailleurs que l'indépendance de l'autorité de contrôle est essentielle, comme le prévoit l'article 7 de la Charte. D'un point de vue pratique, cette manière de procéder entraînerait toutefois un surcroît de travail pour les APD, sans garantie que cette tâche puisse être accomplie en l'absence de moyens supplémentaires. Les APD accueillent donc favorablement le considérant 38 du règlement proposé, qui souligne que chaque autorité de contrôle doit être dotée des ressources financières et humaines, des locaux et des infrastructures supplémentaires nécessaires à l'exécution effective des tâches prévues au titre du nouveau règlement. Le fait que l'article 18, paragraphe 2, établisse la base juridique de la coopération entre les autorités de contrôle du règlement proposé et les autorités de régulation nationales de la proposition de directive établissant le code des communications électroniques européen est également apprécié[5].

6. Compte tenu de la relation étroite existant entre le règlement proposé et le RGPD, **l'alignement des amendes prévues par le règlement proposé sur celles prévues par le RGPD** doit également être salué. Les activités relevant du champ d'application du règlement proposé sont assez sensibles, supposant notamment l'interférence avec les communications confidentielles et l'équipement terminal. Le niveau des amendes doit être proportionné à ce contexte sensible, qui est également la raison pour laquelle l'harmonisation à l'échelle de l'UE est importante, pour assurer le même niveau élevé de protection dans l'ensemble de la région. L'article 23 de la proposition de

[4] Voir par exemple l'arrêt de la CJUE du 6 octobre 2015 dans l'affaire C-362/14 (*sphère de sécurité*), point 41, et l'arrêt de la CJUE du 21 décembre 2016 dans les affaires jointes C-203/15 et C-698/15 (*Tele2/Watson*), point 123.

[5] Proposition de directive du Parlement européen et du Conseil établissant le code des communications électroniques européen (refonte) [2016/0288 (COD), 12.10.2016], url: http://eur-lex.europa.eu/legal-content/FR/ALL/?uri=comnat:COM_2016_0590_FIN.

règlement prévoit des amendes effectives en cas de violation du règlement, d'un niveau identique à celui des amendes fixées en cas de violation des règles du RGPD, sauf pour certains aspects (voir le point 38).

7. La **suppression**, dans ce texte législatif, **de règles spécifiques concernant la notification des violations de données** est également saluée car elle permet d'éviter un chevauchement inutile avec les exigences en matière de violation des données prévues par le RGPD.

8. Le groupe de travail **se félicite** par ailleurs **que la priorité soit à présent accordée à la garantie d'un niveau égal de protection à tous les utilisateurs finaux**, puisque le règlement proposé a supprimé la distinction entre les «abonnés» et les autres utilisateurs de services de communications électroniques.

EXTENSION DU CHAMP D'APPLICATION PAR RAPPORT A LA DIRECTIVE VIE PRIVEE ET COMMUNICATIONS ELECTRONIQUES

9. Le groupe de travail se félicite de **l'extension du champ d'application du règlement proposé pour y inclure les opérateurs proposant des services de communication par contournement («over-the-top», OTT)**; il s'agit de services qui présentent des fonctions équivalentes aux moyens de communication plus traditionnels et peuvent donc avoir un effet similaire sur le respect de la vie privée et le droit à la confidentialité des communications des citoyens de l'UE. Le groupe de travail se félicite notamment que toutes les catégories d'OTT (OTT0, OTT1 et certains OTT2)[6] relèvent à présent du champ d'application du règlement, puisque celui-ci ne couvre pas uniquement les moyens de communication traditionnels (OTT0), mais couvre aussi les services qui présentent des fonctions équivalentes (OTT1) tel qu'indiqué à l'article 8, paragraphe 1, point c), du règlement proposé. Il est par ailleurs positif qu'outre les définitions établies par le code des communications électroniques européen, certains fournisseurs d'OTT2 soient inclus lorsqu'ils fournissent des services de communication interpersonnelle et interactive accessoires intrinsèquement liés à leurs services, comme dans les jeux, les applications de rencontres ou les sites d'avis (article 4, paragraphe 2, de la proposition de règlement). De même, **la précision selon laquelle la protection s'applique également aux interactions de machine à machine** doit également être saluée. Le considérant 12 précise que les dispositifs qui communiquent entre eux relèvent du champ d'application de la protection octroyée par le règlement proposé. Cette protection est souhaitable, étant donné que ces communications contiennent souvent des informations protégées au titre des droits liés au respect de la vie privée. Son applicabilité pourrait toutefois être précisée (voir le point 40 h).

[6] Pour de plus amples explications de ces termes, voir BEREC, *Report on OTT Services*, BoR (16) 35, 29 janvier 2016, pp. 15 et 16, url: http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services. Veuillez noter le commentaire figurant dans le rapport, selon lequel les catégories sont conçues comme des concepts à utiliser dans le débat sur le réexamen, et non comme des concepts juridiques.

10. Il est également positif que **le règlement proposé englobe clairement le contenu et les métadonnées y associées**. Le considérant 14 énonce clairement que la définition des «données de communications électroniques» figurant à l'article 4, paragraphe 3, point a), devrait être formulée de façon suffisamment large pour englober *tout* contenu, ainsi que les métadonnées associées, indépendamment, par exemple, du mode de transmission des signaux. Le groupe de travail note toutefois comme source de préoccupation, au point 39, que la définition actuelle des «données de communications électroniques» reste l'objet d'un débat. Dans l'esprit de l'extension du champ d'application, le groupe de travail estime que **le fait de reconnaître que les métadonnées peuvent révéler des informations très sensibles** (voir point 2.2 de l'exposé des motifs; considérant 2) constitue un ajout essentiel. Le groupe de travail salue le fait que la Commission européenne, en agissant en ce sens, intègre les considérations avancées par la CJUE dans les affaires *Digital Rights Ireland* et *Tele2/Watson*. Le GT29 se félicite également du **constat selon lequel l'analyse du contenu est un traitement qui présente un risque élevé**. Le considérant 19 et l'article 6, paragraphe 3, point b), établissent la présomption juridique logique selon laquelle le balayage du contenu est un traitement qui présente un risque élevé au sens de l'article 35 du RGPD et qui, apparemment indépendamment de l'existence d'un risque élevé résiduel, requiert toujours la consultation préalable de l'autorité (chef de file) chargée de la protection des données. En même temps, le groupe de travail est préoccupé par le champ d'application de la définition des «métadonnées» et par le fait que l'analyse des métadonnées n'est pas soumise à la même obligation de réaliser une analyse d'impact relative à la protection des données (voir les points 33 et 46).

11. Le groupe de travail se félicite également du maintien de la **reconnaissance de l'importance de l'anonymisation.** Dans la directive vie privée et communications électroniques, les mesures d'anonymisation contribuaient déjà à assurer la compatibilité (par exemple l'article 6, paragraphe 1, de la directive, aux termes duquel les données relatives au trafic doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication). L'article 6, paragraphe 2, point c), et l'article 6, paragraphe 3, point b), du règlement proposé prévoient une exception à l'interdiction du traitement des métadonnées et du contenu, subordonnée au consentement de l'utilisateur final, «*à condition que le traitement d'informations anonymisées ne permette pas d'atteindre*» les objectifs considérés. L'instauration obligatoire de ce type de mesures de protection, en plus du consentement des utilisateurs, protège ces derniers d'un traitement injustifié. Toutefois, le groupe de travail est en même temps fortement préoccupé par le fait que l'adoption de telles techniques d'anonymisation ne serait pas requise lors du suivi de la localisation des utilisateurs au moyen de leurs appareils mobiles (voir le point 17). En outre, même en cas d'application de mesures d'anonymisation, les fournisseurs devraient toujours réaliser une analyse d'impact relative à la protection des données (voir les points 33 et 46), et le groupe de travail demande une obligation supplémentaire imposant de rendre publique la méthode d'anonymisation et d'agrégation (voir le point 42 b).

12. La **formulation très vaste de la protection de l'équipement terminal** constitue un autre point positif. Le considérant 20 et l'article 8 disposent que les technologies

utilisées pour avoir accès à l'équipement terminal n'ont pas d'importance: toute interférence avec l'équipement terminal, y compris le recours aux capacités de traitement de celui-ci, requiert le consentement de l'utilisateur final (avec certaines exceptions). La CE a désormais utilement confirmé que la «capture d'empreintes numériques» relève de ladite disposition. Le groupe de travail se félicite en outre que les préférences définies dans les **paramètres du navigateur** de la personne **soient opposables** à un tiers, comme indiqué au considérant 22. Cette opposabilité sera utile en cas de non-respect de ces paramètres par un tiers (par exemple un réseau publicitaire). Cependant, elle doit également être énoncée dans une disposition pertinente du règlement proposé.

13. Enfin, le groupe de travail salue la poursuite de l'**inclusion des personnes morales dans le champ d'application du règlement proposé** (voir point 2.2 de l'exposé des motifs; considérants 3, 33 et 42; articles 1 et 15 et article 16, paragraphe 5). C'est déjà le cas pour la directive vie privée et communications électroniques; toutefois, étant donné que les autorités chargées de la protection des données seront responsables du contrôle de l'application des nouvelles règles, il est utile de le souligner spécifiquement. Les autorités chargées de la protection des données pourront ainsi prendre des mesures dans les cas où des personnes morales sont victimes d'une infraction, par exemple lorsque des entreprises reçoivent des courriels indésirables ou que leurs communications sont contrôlées subrepticement. Cependant, le groupe de travail relève également comme source de préoccupation le fait que l'application du consentement aux personnes morales n'est pas claire (voir le point 41 a), de même que la signification de la notion d'«intérêt légitime» des personnes morales en cas de prospection directe (voir le point 43 c).

APPLICATION CIBLEE DE LA NOTION DE CONSENTEMENT

14. Le groupe de travail accueille favorablement une autre catégorie d'améliorations concernant l'application et l'interprétation de la notion de consentement, et en premier lieu **la précision concernant le fait que l'accès à l'internet et la téléphonie (mobile) sont des services essentiels et que les fournisseurs de ces services ne peuvent «obliger» leurs clients à consentir à un traitement de données qui n'est pas nécessaire à la fourniture de ces services eux-mêmes**. Au considérant 18 notamment, il est indiqué que l'accès à l'internet à haut débit de base et les services de communications vocales doivent être considérés comme des services essentiels, ce qui signifie, compte tenu de la dépendance des individus à l'accès à ces services, que le consentement au traitement de leurs données de communications à des fins supplémentaires (par exemple à des fins de publicité ou de prospection) ne peut être valable. En même temps, le groupe de travail s'inquiète du fait que cette précision est trop limitée. Les services de certains fournisseurs de services OTT peuvent également être considérés comme des services essentiels et le règlement relatif à la vie privée et aux communications électroniques devrait aussi interdire de manière explicite les choix «à prendre ou à laisser» dans d'autres circonstances (voir le point 20).

15. Il est également positif que **l'obligation de consentement pour l'enregistrement des données à caractère personnel de personnes physiques dans des annuaires soit harmonisée**. En vertu de l'article 15 du règlement proposé, le traitement des données dans les annuaires publics n'est permis qu'avec le consentement des personnes physiques et la possibilité, pour les personnes morales, de s'y opposer. Ce point est expliqué plus en détail au considérant 31, qui indique que ce consentement doit être spécifique en ce qui concerne les catégories particulières de données à caractère personnel qui peuvent figurer dans l'annuaire. Le groupe de travail note toutefois comme source de préoccupation que la proposition de règlement pourrait indiquer plus clairement qu'un consentement spécifique distinct sera requis pour les fonctions de recherche et de recherche inverse (voir le point 37).

16. **La nouvelle exception ciblée concernant l'interférence non intrusive avec l'équipement terminal** est également appréciée. Le GT29 juge utile que le règlement proposé précise que l'interdiction ne s'applique pas à la mesure du trafic sur un site web [en vertu de l'exception restrictive selon laquelle cette mesure doit être effectuée par le fournisseur du service de la société de l'information demandé par l'utilisateur final, voir l'article 8, paragraphe 1, point d), de la proposition de règlement]. Voir également le considérant 21. Le groupe de travail suggère toutefois d'utiliser une définition plus neutre du point de vue technologique et de préciser l'applicabilité de cette exception (voir le point 25).

3. SOURCES DE PRÉOCCUPATION MAJEURE

LA PROTECTION ACCORDEE AU TITRE DU RGPD EST COMPROMISE PAR LE REGLEMENT PROPOSE

Comme indiqué plus haut, la proposition de règlement apporte un certain nombre d'améliorations essentielles. Elle renferme toutefois également des sources de

préoccupation majeure, à des degrés de gravité divers. Dans la présente partie, le groupe de travail examine les quatre points qu'il juge **extrêmement préoccupants**. Il s'agit de dispositions qui **compromettent le niveau de protection accordé par le RGPD**.

17. **Les obligations énoncées dans le règlement concernant le suivi de la localisation de l'équipement terminal doivent respecter les exigences établies par le RGPD**. L'article 8, paragraphe 2, point b), impose uniquement l'affichage d'un message et la mise en œuvre de mesures de sécurité pour la collecte des informations émises par l'équipement terminal. Il précise en outre que la personne qui est responsable de la collecte des informations doit indiquer les mesures éventuelles que peuvent prendre les utilisateurs finaux pour réduire au minimum la collecte ou la faire cesser. Ce faisant, l'article 8, paragraphe 2, point b), donne l'impression que les organisations peuvent collecter les informations émises par l'équipement terminal pour suivre les mouvements physiques des personnes (comme le «suivi par Wi-Fi» ou le «suivi par Bluetooth») sans le consentement de la personne concernée. La partie collectant ces données pourrait apparemment satisfaire aux exigences au moyen d'un message indiquant aux utilisateurs d'éteindre leurs appareils lorsqu'ils ne souhaitent pas faire l'objet d'un suivi. Ce type d'approche serait contraire à l'objectif fondamental de la politique des télécommunications de la Commission européenne, qui vise à fournir une connectivité à l'internet mobile à haut débit assurant à tous les Européens, par-delà les frontières, une protection élevée de la vie privée à un faible coût.

En outre, le règlement proposé n'impose aucune limitation claire en ce qui concerne le champ d'application de la collecte des données ou des activités de traitement ultérieures. Dans ce contexte, il y a lieu de noter que les adresses MAC sont des données à caractère personnel, y compris après la mise en œuvre de mesures de sécurité telles que le hachage. En l'absence de toute exigence ou limitation supplémentaire, le niveau de protection de ces données à caractère personnel par le règlement proposé est considérablement inférieur à celui fixé par le RGPD, conformément auquel ce type de suivi devrait être loyal, légal et transparent. Le considérant 25 indique en outre, de manière assez malheureuse, que certaines fonctionnalités de suivi par Wi-Fi ne comportent pas de risques importants pour la vie privée, à l'inverse d'autres, comme celles qui impliquent le suivi de personnes dans le temps. Si le groupe de travail se réjouit que cette dernière activité soit reconnue comme comportant des risques importants pour la vie privée, il estime qu'il n'est pas opportun de décider d'emblée que certaines fonctionnalités n'en comportent pas, sans autre évaluation des circonstances dans lesquelles se déroule le traitement et de sa proportionnalité. Pour la réalisation de cette évaluation, les conditions ci-après concernant le suivi par Wi-Fi non anonymisé devraient être prises en considération.

En fonction des circonstances et des finalités de la collecte de données, dans le cadre du RGPD, le suivi est susceptible soit d'être soumis au consentement, soit de ne pouvoir être effectué que si les données à caractère personnel sont anonymisées. Cette anonymisation s'effectue de préférence immédiatement après la collecte. Si ce n'est pas possible compte tenu de la finalité de la collecte des données, celles-ci peuvent être traitées au cours d'une période où elles ne sont pas anonymisées uniquement dans les conditions suivantes: i) la finalité de la collecte de données doit se limiter à un simple comptage statistique (voir les exemples ci-dessous), ii) le suivi doit être limité dans l'espace et dans le temps à ce qui est strictement nécessaire à la réalisation de cette finalité, iii) les données doivent être supprimées ou anonymisées immédiatement après le traitement et iv) il doit exister une possibilité effective de

refuser cette collecte. Dans tous les cas, les responsables du traitement doivent évidemment respecter l'exigence relative à la fourniture d'informations appropriées.

Le groupe de travail est préoccupé par le fait qu'un système dans lequel l'utilisateur devrait refuser le suivi de manière individuelle pour chaque organisation collectant ces données ferait peser une charge inacceptable sur les citoyens, étant donné la croissance du déploiement de ces technologies de suivi tant par les organisations du secteur privé que par celles du secteur public. Par conséquent, le groupe de travail appelle le législateur européen à encourager l'élaboration de normes techniques permettant aux dispositifs de signaler automatiquement une objection à ce type de suivi et à faire en sorte que ce signal soit contraignant.

Par exemple, il est probable qu'un consentement au titre du RGPD soit requis lorsqu'un responsable du traitement collecte et stocke les adresses MAC (Wi-Fi ou Bluetooth) de dispositifs, indirectement identifiables, et calcule la localisation de l'utilisateur, afin de suivre sa position au cours du temps, par exemple dans divers magasins. C'est en particulier le cas lorsque ce suivi a lieu dans des espaces publics, où les utilisateurs peuvent légitimement s'attendre à ne pas être identifiés ni suivis, mais où les adresses MAC des passants sont collectées. Ce consentement pourrait par exemple être obtenu au moyen d'une application invitant les utilisateurs à autoriser le suivi de leur position dans une zone déterminée en échange d'offres commerciales, ou grâce à des points d'enregistrement à l'intérieur de certains lieux, ou encore par l'intermédiaire d'un module de consentement lié aux points d'accès sans fil.

Les situations dans lesquelles les responsables du traitement peuvent être autorisés à traiter les informations émises par les équipements terminaux aux fins du suivi des mouvements physiques d'individus sans le consentement de ces derniers sont limitées. Ce pourrait par exemple être le cas lors du comptage du nombre de clients en un lieu précis ou lors de la collecte des données émises des deux côtés d'un poste de sécurité pour afficher le temps d'attente. Toutefois, dans ces deux exemples, les données devraient être supprimées ou anonymisées dès la finalité statistique accomplie. Cela signifie que les adresses MAC des dispositifs des visiteurs présents en un lieu déterminé, comme un magasin, doivent être anonymisées immédiatement après la collecte, sans aucun stockage permanent et de manière à ce qu'il soit techniquement impossible de les réidentifier. Dans le cas d'un calcul de temps d'attente, les adresses MAC doivent être supprimées ou anonymisées dès que les données ne sont plus pertinentes aux fins du calcul (par exemple parce que le visiteur est passé de l'autre côté du poste de sécurité ou parce qu'il a quitté la file d'attente).
En outre, le responsable du traitement doit respecter les exigences visant à réduire au minimum la collecte de données (par exemple, pas de suivi 24 heures sur 24 si la finalité est limitée aux heures d'ouverture du magasin et/ou échantillonnage à intervalles réguliers). Les responsables du traitement doivent également prendre d'autres mesures d'atténuation pour veiller à ce qu'il n'y ait pas ou guère d'incidence sur les droits des utilisateurs au respect de la vie privée, par exemple pour protéger la vie privée de personnes vivant à proximité d'un point de collecte.

Le choix de l'exigence d'un simple avertissement, opéré à l'article 8, paragraphe 2, du règlement proposé, est d'autant plus étonnant que le considérant 20 conclut que la

collecte d'informations relatives au dispositif de l'utilisateur final aux fins de l'identification et du suivi est également possible à distance et que ce traitement peut, selon le règlement proposé, porter gravement atteinte à la vie privée de l'utilisateur concerné. De plus, l'obligation ne va pas au-delà de l'obligation d'information déjà établie aux articles 13 et 14 du RGPD. L'atteinte grave à la vie privée que représente le suivi est encore aggravée par l'accès potentiel d'autres personnes aux données collectées ; les services répressifs ont par exemple la possibilité d'identifier les utilisateurs finaux sur la base des adresses MAC stockées émises par les dispositifs mobiles de ces utilisateurs.

18. **Les conditions dans lesquelles l'analyse du contenu et des métadonnées est autorisée doivent être développées.**

L'article 6 du règlement proposé prévoit des niveaux de protection différents pour les métadonnées et le contenu. Le GT29 ne soutient pas cette différenciation: les deux catégories de données sont hautement sensibles. Les métadonnées et le contenu devraient donc bénéficier du même niveau élevé de protection. Le point de départ devrait par conséquent être l'interdiction de traiter les métadonnées ainsi que le contenu sans le consentement de tous les utilisateurs finaux (c'est-à-dire l'émetteur et le destinataire).

Toutefois, selon les fins recherchées, certains types de traitement peuvent être autorisés sans consentement, si cela est strictement nécessaire auxdites fins:

- Les fournisseurs peuvent traiter des données de communications électroniques aux fins visées à l'article 6, paragraphe 1, points a) et b), et à l'article 6, paragraphe 2, points a) et b), du règlement proposé[7].
- Il convient de préciser que certaines techniques de détection/de filtrage du pollupostage et de lutte contre les réseaux zombies peuvent également être considérées comme strictement nécessaires pour détecter ou faire cesser les fraudes à l'usage des services de communications électroniques [article 6, paragraphe 2, point b)]. En ce qui concerne le pollupostage, les utilisateurs recevant ce type de communications devraient se voir offrir, lorsque cela est techniquement réalisable, des possibilités d'opposition granulaire.
- Il convient de préciser que l'analyse des données de communications électroniques à des fins de service aux clients peut également relever de l'exception relative à la nécessité d'établir des factures [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 facture peut être légalement contestée ou des poursuites peuvent être engagées pour en

[7] En ce qui concerne la nécessité de satisfaire aux prescriptions obligatoires en matière de qualité de service, comme indiqué à l'article 6, paragraphe 2, point a), du règlement proposé, les fournisseurs devraient tenir compte des conditions énoncées dans le règlement (UE) 2015/2120 (code des communications électroniques européen), et en particulier de l'article 3 et des considérants 10 et 13 à 15. Sur la base de cette disposition, les fournisseurs peuvent être tenus de traiter des données de communications pour détecter et filtrer les logiciels malveillants et les logiciels espions, et ils peuvent être autorisés à compresser les données.

obtenir le paiement en application du droit national. Les données pertinentes (comme les url) ne peuvent être conservées qu'à la demande de l'utilisateur final et uniquement pendant la période strictement nécessaire à la résolution d'un litige concernant une facture (ce qui signifie que l'article 7, paragraphe 3, devrait être modifié).

- Il devrait être rendu possible de traiter les données de communications électroniques en vue de la fourniture de services explicitement demandés par un utilisateur final, comme les fonctions de recherche et d'indexation de mots-clés, les assistants virtuels, les moteurs de synthèse vocale et les services de traduction. À cette fin, il est nécessaire d'introduire une exemption concernant l'analyse de ces données pour les usages purement individuels (domestiques), ainsi que les usages professionnels individuels[8]. Cette analyse serait ainsi possible sans le consentement de tous les utilisateurs finaux, mais ne pourrait avoir lieu qu'avec le consentement de l'utilisateur final demandant le service. Ce consentement spécifique empêcherait également le fournisseur d'utiliser ces données à des fins différentes.

Ce qui précède signifie que l'exploitation du contenu et/ou des métadonnées à toute autre fin, comme l'analyse, le profilage, la publicité comportementale ou d'autres fins procurant un avantage (commercial) au fournisseur, requiert le consentement de tous les utilisateurs finaux dont les données seraient traitées. En ce qui concerne ces situations, le règlement proposé devrait indiquer que le simple fait d'envoyer un courrier électronique ou une autre forme de communication personnelle depuis un autre service à un utilisateur final qui a personnellement consenti au traitement du contenu et des métadonnées le concernant (par exemple lors de l'inscription à un service de courrier électronique) ne constitue pas un consentement valable de la part de l'émetteur.

Enfin, il convient de préciser que le traitement de données concernant des personnes autres que les utilisateurs finaux (par exemple une photographie ou une description d'un tiers dans un échange entre deux personnes) suppose également la nécessité de respecter toutes les dispositions pertinentes du RGPD.

19. **L'équipement terminal et les logiciels doivent *par défaut* décourager, prévenir et interdire les interférences illégales avec eux et fournir des informations sur les possibilités offertes à cet égard**. Bien que le règlement proposé oblige les fournisseurs de logiciels mis sur le marché qui permettent d'effectuer des communications électroniques à offrir «la possibilité» d'empêcher une forme limitée d'interférence avec l'équipement terminal et, au moment de l'installation, contraigne les fournisseurs de logiciels à imposer à l'utilisateur final de donner son

[8] Si le considérant 13 du règlement proposé exclut explicitement les réseaux d'entreprise du champ d'application du règlement, cette nouvelle exception concernant l'usage individuel devrait également couvrir l'utilisation de services en nuage par les employés à des fins professionnelles, par exemple la recherche dans leurs courriers électroniques.

consentement à un paramètre de confidentialité (article 10, paragraphes 1 et 2), ce choix n'équivaut pas au *respect de la vie privée par défaut*. En outre, la «possibilité» d'empêcher certaines interférences existe déjà et, à ce jour, elle n'a pas permis de remédier de manière satisfaisante au problème du suivi non justifié. C'est précisément pour cette raison que, dans le cadre du RGPD, le législateur a consciemment fait le choix stratégique d'introduire les principes de protection des données dès la conception et de protection des données par défaut (article 25 du RGPD). Le règlement proposé compromet ces principes en ce qui concerne les données de communications et les données des dispositifs. Dans le même temps, la directive 2014/53/UE[9] sur les équipements radioélectriques (mentionnée au considérant 10) ne prévoit qu'une obligation très limitée en matière de sécurité, exigeant que les équipements radioélectriques «comportent des sauvegardes afin d'assurer la protection des données à caractère personnel et de la vie privée des utilisateurs et des abonnés» [article 3, paragraphe 3, point e)]. Cette obligation ne peut remplacer les paramètres spécifiques de respect de la vie privée par défaut au titre du règlement proposé. À cet égard, il convient également de souligner que, selon l'enquête Eurobaromètre sur la vie privée et les communications électroniques publiée en décembre 2016, près de sept répondants sur dix (69 %) sont tout à fait d'accord avec l'affirmation selon laquelle les paramètres par défaut de leur navigateur devraient empêcher le partage de leurs informations[10]. Le groupe de travail nourrit par ailleurs des préoccupations en ce qui concerne les paramètres des navigateurs et la définition des «tiers». Voir le point 24. De plus, il convient de garder à l'esprit que cette disposition ne concerne pas uniquement les navigateurs utilisés sur les ordinateurs, mais aussi les autres types de logiciels qui permettent des communications (y compris les systèmes d'exploitation, applications et interfaces logicielles pour les dispositifs connectés à l'internet des objets). En résumé, les équipements terminaux et les logiciels doivent, *par défaut*, offrir des paramètres assurant la protection de la vie privée, et guider vers le menu de configuration l'utilisateur qui souhaite s'écarter de ces paramètres par défaut lors de l'installation. Le menu de configuration devrait toujours être facilement accessible au cours de l'utilisation. Le groupe de travail encourage le législateur européen à clarifier le champ d'application de l'article 10 en ce sens.

20. **Le règlement relatif à la vie privée et aux communications électroniques devrait explicitement interdire les *tracking walls***, c'est-à-dire la pratique consistant à interdire l'accès à un site web ou à un service à moins que l'utilisateur ne consente à faire l'objet d'un suivi sur d'autres sites web ou services. Comme le groupe de travail l'a déjà indiqué dans ses précédents avis sur la directive vie privée et communications électroniques[11], les approches «à prendre ou à laisser» de ce type sont rarement

[9] Directive 2014/53/UE sur les équipements radioélectriques.

[10] Voir le rapport Eurobaromètre Flash 443 sur la vie privée et les communications électroniques (publié en décembre 2016), p. 5.

[11] Voir, par exemple, le WP 240 (réexamen de la directive vie privée et communications électroniques), p. 16, et le WP 208 (exceptions au consentement), p. 5.

légitimes[12]. Lorsque l'utilisation des capacités de traitement et de stockage de l'équipement terminal ou la collecte d'informations à partir de l'équipement terminal des utilisateurs finaux permettent le suivi des activités des utilisateurs à travers le temps ou dans le cadre de plusieurs services (par exemple différents sites web ou applications), ces activités de traitement peuvent constituer une intrusion grave dans la vie privée des utilisateurs concernés. Étant donné le rôle primordial joué par l'internet dans l'exercice du droit fondamental à la liberté d'expression, y compris le droit d'accès à l'information, la capacité des utilisateurs à accéder au contenu en ligne ne devrait pas dépendre de l'acceptation du suivi de leurs activités sur différents dispositifs et sites web/applications. Le futur règlement relatif à la vie privée et aux communications électroniques devrait par conséquent préciser que l'accès au contenu, par exemple, sur les sites web et les applications ne peut être subordonné à l'acceptation de ce type d'activités de traitement intrusives, indépendamment de la technologie de suivi appliquée, comme les cookies, la capture d'empreintes numériques, l'utilisation d'identifiants uniques ou d'autres techniques de suivi. La nécessité de cette interdiction ressort de la récente enquête Eurobaromètre sur la vie privée et les communications électroniques, qui a montré que près de deux tiers (64 %) des répondants estiment inacceptable que leurs activités en ligne soient suivies en échange d'un accès sans entrave à certains sites web.

21. En résumé, en ce qui concerne les quatre points exposés ci-dessus, **le règlement proposé devrait respecter sa promesse d'offrir un niveau de protection égal ou supérieur au RGPD**. En son considérant 5, il est affirmé sobrement que le règlement proposé n'abaisse pas le niveau de protection offert par le RGPD. Toutefois, tel que ce règlement se présente actuellement, cette affirmation est erronée, en particulier en ce qui concerne le suivi des dispositifs (point 17), l'absence du principe de respect de la vie privée par défaut (point 19) et le consentement (point 18). Cela est particulièrement pertinent étant donné qu'il est indiqué, dans le même considérant, que le règlement proposé «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». Le groupe de travail suggère que le texte du règlement relatif à la vie privée et aux communications électroniques précise au moins ce qui suit:

    i) les interdictions établies par le règlement relatif à la vie privée et aux communications électroniques priment sur les autorisations accordées en vertu du RGPD [par exemple l'interdiction d'interférence établie à l'article 5 du règlement relatif à la vie privée et aux communications électroniques prime sur les droits des fournisseurs de services de communications électroniques de procéder au traitement ultérieur des données à caractère personnel en vertu de l'article 5, paragraphe 1, point b), et de l'article 6, paragraphe 4, du RGPD];

    ii) lorsque le traitement est autorisé au titre d'une des exceptions (y compris le consentement) aux interdictions établies par le règlement relatif à la vie privée et aux communications électroniques, ce traitement, lorsqu'il concerne

[12] Cette position est sans préjudice de l'article 7, paragraphe 4, du RGPD, qui peut également empêcher les choix «à prendre ou à laisser» dans d'autres situations, lorsque cela est approprié.

des données à caractère personnel, doit rester conforme à l'ensemble des dispositions du RGPD;

iii) lorsque le traitement est autorisé au titre d'une des exceptions aux interdictions établies par le règlement relatif à la vie privée et aux communications électroniques, tout autre traitement en vertu du RGPD est interdit, y compris le traitement à une fin autre que celle pour laquelle les données ont été collectées au titre de l'article 6, paragraphe 4, du RGPD. Cela n'empêcherait toutefois pas les responsables du traitement de demander un consentement supplémentaire pour de nouvelles opérations de traitement, pas plus que les législateurs de prévoir des exceptions supplémentaires limitées et spécifiques dans le règlement relatif à la vie privée et aux communications électroniques, par exemple pour autoriser le traitement des données à des fins scientifiques ou statistiques au titre de l'article 89 du RGPD ou pour sauvegarder les «intérêts vitaux» des personnes en vertu de l'article 6, point d), du RGPD.

En outre, le règlement relatif à la vie privée et aux communications électroniques devrait être interprété de manière à ce qu'il accorde un niveau de protection au moins équivalent et, si cela est approprié, supérieur à celui offert par le RGPD.

4. AUTRES POINTS DE PRÉOCCUPATION

Outre les points mentionnés ci-dessus, le groupe de travail «Article 29» est **préoccupé** par les éléments ci-après.

LE CHAMP D'APPLICATION TERRITORIAL ET MATERIEL DOIT ETRE ETENDU

22. **Le terme «métadonnées» est défini de manière trop restreinte**. Ce terme est actuellement défini à l'article 4, paragraphe 3, point c), comme «les données traitées dans un réseau de communications électroniques aux fins de la transmission, la distribution ou l'échange de contenu de communications électroniques» (soulignement ajouté). L'utilisation du terme «réseau» semble indiquer que seules les données générées au cours de la fourniture de services dans la couche «inférieure» du réseau seraient des «métadonnées», ce qui pourrait signifier que les données générées lors de la fourniture d'un service OTT seraient exclues de ce champ d'application. Cela ne serait pas souhaitable, et n'est probablement pas délibéré, étant donné l'intention d'élargir le champ d'application du règlement proposé aux fournisseurs de services OTT. Afin de remédier à cette situation, il convient de modifier la définition des «métadonnées de communications électroniques» pour y inclure toutes les données traitées aux fins de la transmission, de la distribution ou de l'échange de contenu de communications électroniques.

23. Est également source de préoccupation le fait que **le champ d'application territorial du règlement proposé en ce qui concerne les organisations ne disposant pas d'établissement dans l'Union ne couvre que les fournisseurs de services de communications électroniques**. Au titre du règlement proposé, le fournisseur d'un service de communications électroniques qui n'est pas établi dans l'Union désigne par écrit un représentant dans l'Union (article 3, paragraphe 2). Il est également

mentionné, au considérant 9, que le règlement devrait s'appliquer aux traitements effectués par les fournisseurs de services de communications électroniques indépendamment de l'endroit où a lieu le traitement. Le groupe de travail salue cette précision. Néanmoins, étant donné que le libellé est limité aux fournisseurs de services de communications électroniques, on ne sait pas avec certitude dans quelle mesure ce champ d'application territorial s'applique également aux autres parties [par exemple les parties collectant les informations diffusées par l'équipement terminal des utilisateurs finaux ou interférant avec ces informations, voir l'article 3, paragraphe 1, point c), lu conjointement avec l'article 8 du règlement proposé]. Par conséquent, le groupe de travail suggère de modifier l'article 3, paragraphes 2 et 5, afin d'inclure les fournisseurs d'annuaires accessibles au public, les fournisseurs de logiciels permettant des communications électroniques et les personnes envoyant des communications commerciales de prospection directe ou recueillant des informations (d'autre nature) qui concernent l'équipement terminal de l'utilisateur final ou qui y sont stockées, lorsque leurs activités ciblent des utilisateurs dans l'Union (voir le considérant 8 du règlement proposé)[13].

LA PROTECTION DE L'EQUIPEMENT TERMINAL DOIT ETRE RENFORCEE

L'insuffisance de la protection de l'équipement terminal prévue par le règlement proposé soulève une autre série de préoccupations.

24. Premièrement, **le règlement proposé laisse penser, à tort, qu'un consentement valable peut être donné par l'intermédiaire des paramètres non spécifiques des navigateurs**. Le groupe de travail reconnaît que les utilisateurs finaux sont actuellement débordés par les demandes de consentement (considérant 22). Les paramètres des navigateurs (et des logiciels comparables) ont un rôle important à jouer pour remédier à ce problème. Toutefois, étant donné que les paramètres généraux des navigateurs n'ont pas vocation à s'appliquer à l'utilisation d'une technologie de suivi dans un cas particulier, ils ne se prêtent pas à l'octroi du consentement au titre de l'article 7 et du considérant 32 du RGPD (le consentement n'étant ni éclairé ni suffisamment spécifique).
L'utilisateur final doit être en mesure de donner distinctement par site web ou par application son consentement au suivi à différentes fins (comme le partage sur les médias sociaux ou la publicité). Un responsable du traitement chargé de plusieurs sites web ou applications peut également demander un consentement pour l'ensemble des sites ou applications qu'il contrôle, pour autant que cette demande de consentement soit présentée séparément.

[13] Voir l'article 3, paragraphe 2, du RGPD: «*Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées: a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes; ou b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.*» Cette obligation pourrait également être assortie d'exceptions sur le modèle de l'article 27, paragraphe 2, du RGPD.

En outre, le responsable du traitement doit respecter toutes les autres obligations liées au consentement, y compris l'obligation de fournir des informations adéquates aux utilisateurs. Pour les navigateurs comme pour les responsables du traitement, cela signifie que le consentement ne serait pas valable s'ils n'offraient que la possibilité d'accepter tous les cookies, étant donné que cela ne permettrait pas aux utilisateurs de donner leur consentement avec la granularité requise. Toutefois, il devrait être possible pour les navigateurs d'autoriser les utilisateurs à effectuer un choix éclairé et conscient visant à accepter tous les cookies, et donc à empêcher toute demande de consentement future spécifique de la part des sites web qu'ils visitent.

Le groupe de travail recommande fortement que le règlement relatif à la vie privée et aux communications électroniques rende obligatoire la mise en œuvre de mesures techniques telles que la norme *Do Not Track* (DNT) dans les navigateurs, pour veiller à ce que les utilisateurs se voient offrir un choix et un contrôle réels en ce qui concerne les interférences avec leurs dispositifs[14].

Plus important encore, il convient que le règlement relatif à la vie privée et aux communications électroniques garantisse que le choix concernant le stockage d'informations sur le dispositif et un signal DNT provenant d'un navigateur soient tous deux acceptés comme une indication juridiquement contraignante du consentement ou du refus de l'utilisateur par l'ensemble des responsables du traitement. Ce qui précède est sans préjudice d'autres orientations qui seront fournies par le groupe de travail concernant la conformité de la norme DNT avec, notamment, le principe de limitation des finalités lorsque la norme aura été finalisée (finalisation prévue pour la fin de 2017).

Les types de consentement «implicites», comme le fait de cliquer sur le site web ou de faire défiler la page, ne peuvent supplanter les choix concernant le stockage et le signal DNT. Un avantage important de l'utilisation de cette norme réside dans le fait qu'elle ne se limite pas à la technologie de suivi par cookies, mais couvre également d'autres types de suivi, comme la capture d'empreintes.

Le fait de rendre l'adhésion à cette norme juridiquement obligatoire permettra également de résoudre un autre problème, lié à l'utilisation actuelle, à l'article 10, du terme «tiers». Une page web ou une application contient généralement de nombreux éléments, provenant du site web lui-même ou externes. Un code externe peut également être exécuté sur le site web visité et contacter le serveur d'un tiers. Un cookie traceur peut être utilisé par le propriétaire d'un site, par exemple, de socialisation lorsqu'un utilisateur visite ce site. Ce site de socialisation peut également agir comme tiers lorsque cet utilisateur consulte un autre site web qui contient des interactions avec le site de socialisation. Dans tous ces cas, qu'il s'agisse d'accès à l'information ou de stockage d'informations sur le dispositif de l'utilisateur final, il y a interférence avec le dispositif, ce qui requiert un consentement (à moins qu'une des exceptions ne s'applique). La norme DNT résout ce problème en utilisant les termes «*site-wide*» (à l'échelle du site) et «*internet-wide*» (à l'échelle de l'internet). Par conséquent, afin d'améliorer la sécurité juridique pour toutes les parties prenantes, la référence aux «tiers» figurant dans le règlement relatif à la vie

[14] Voir l'url: https://www.w3.org/TR/tracking-compliance/. Le paragraphe 7 expose le modèle d'exception et explique la différence entre les exceptions à l'échelle d'un site et les exceptions à l'échelle du web. Le paragraphe 6 indique les informations lisibles par machine que les responsables du traitement peuvent fournir en ce qui concerne les exigences d'information en vue d'obtenir le consentement.

privée et aux communications électroniques devrait être reformulée pour couvrir toutes les entités avec lesquelles un dispositif interagit (du fait du stockage d'informations sur le dispositif ou de l'accès à l'information stockée sur ce dernier).

Afin de rendre la norme *Do Not Track* compatible avec le niveau élevé de protection de la confidentialité des communications et de protection des données octroyé par la Charte, le règlement relatif à la vie privée et aux communications électroniques devrait préciser que les demandes de suivi à l'échelle de l'internet, par opposition au suivi à l'échelle du site web, doivent être présentées séparément et que les utilisateurs doivent être libres d'accepter ou de refuser ces demandes. En outre, pour protéger les utilisateurs des demandes de consentement fréquentes, le règlement relatif à la vie privée et aux communications électroniques devrait veiller à ce que le refus du suivi à l'échelle de l'internet pour une organisation spécifique (par l'intermédiaire de la norme DNT ou d'une liste noire distincte) empêche cette organisation de formuler de nouvelles demandes de consentement pendant au moins six mois. Cette règle n'empêche pas cette organisation, lorsque son site est visité directement par l'utilisateur (c'est-à-dire lorsqu'elle n'agit pas en tant que tiers), de demander le consentement sur son propre site web (c'est-à-dire une demande de consentement à l'échelle du site). Dans la pratique, cela signifie, par exemple, qu'un site de diffusion de vidéos en continu qui utilise des cookies traceurs peut demander le consentement de l'utilisateur lorsque celui-ci visite le site, mais ne peut pas redemander ce consentement pendant une période de six mois lorsque cet utilisateur a refusé le consentement et visite d'autres sites web qui contiennent des vidéos diffusées depuis le site de diffusion en continu.

25. Par ailleurs, **l'exception concernant la mesure des résultats d'audience sur le web est formulée de manière imprécise**. L'article 8, paragraphe 1, point d), du règlement proposé prévoit une exception pour la mesure des résultats d'audience sur le web. Le premier point de préoccupation concerne le fait que ce terme n'est pas défini et peut être confondu avec le profilage des utilisateurs. La définition devrait indiquer clairement que cette exception ne peut pas être utilisée à des fins de profilage quelles qu'elles soient. L'exception ne doit s'appliquer qu'à l'analyse de l'usage nécessaire aux fins de l'appréciation de la performance du service demandé par l'utilisateur, mais pas à l'analyse des utilisateurs (c'est-à-dire l'analyse du comportement d'utilisateurs identifiables d'un site web, d'une application ou d'un dispositif). Par conséquent, l'exception ne peut être utilisée dans les situations où les données peuvent être reliées aux données d'utilisateurs identifiables traitées par le fournisseur ou par d'autres responsables du traitement. De plus, cette description semble indiquer une application fortement liée à une technologie particulière. Il convient donc de redéfinir le terme «mesure des résultats d'audience sur le web» d'une manière neutre du point de vue technologique, afin de couvrir également une utilisation analytique similaire d'informations obtenues à partir d'applications, de dispositifs portables et de dispositifs liés à l'internet des objets.

Le groupe de travail suggère que l'on s'inspire de l'exception néerlandaise, qui ne s'applique que si elle est strictement nécessaire à l'obtention d'informations relatives à la qualité technique ou à l'efficacité d'un service de la société de l'information et qu'elle n'a pas d'incidence sur le respect de la vie privée de l'abonné ou de

l'utilisateur final concernés [voir l'article 11.7a(3)(b) de la loi néerlandaise sur les télécommunications]. Cette exception tient compte du fait que la plupart des données collectées par l'intermédiaire de l'analyse des sites web ou des applications restent des données à caractère personnel, ce qui signifie que le traitement de ces données est également soumis au RGPD. Il en découle que l'analyse de l'usage peut être réalisée par une organisation externe uniquement si:
i) cette organisation agit en tant que sous-traitant;
ii) un contrat de sous-traitance conforme au RGPD est conclu;
iii) la technologie d'analyse utilisée empêche toute réidentification, y compris, notamment, l'anonymisation de l'adresse IP des utilisateurs;
iv) le ou les cookies spécifiques ou autres données utilisés aux fins de l'analyse ne peuvent servir que pour le site, l'application ou le dispositif portable considéré et ne peuvent être reliés à d'autres données identifiables;
v) les utilisateurs ont le droit de s'opposer à la collecte de données (voir également les points 17 et 50 du présent avis).

Même si le consentement n'est pas requis lorsque ces conditions sont remplies, les responsables du traitement n'en restent pas moins tenus de fournir des informations adéquates aux utilisateurs, par exemple au moyen des champs consacrés à la représentation du statut du suivi (*tracking status representation*) dans la norme *Do Not Track*[15].

26. Le règlement relatif à la vie privée et aux communications électroniques **devrait veiller à ce que les exceptions aux exigences en matière de consentement soient de portée restreinte et formulées de manière précise**. Le libellé de l'exception à l'exigence de consentement pour l'interférence avec les dispositifs établie à l'article 8, paragraphe 1, point c), est pratiquement identique au libellé actuel de l'article 5, paragraphe 3, de la directive vie privée et communications électroniques («*strictement nécessaires au fournisseur pour la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur*»), mais le terme essentiel «strictement» a été omis, sans explication. Cette omission est préoccupante pour deux raisons. Tout d'abord, la disposition de la directive vie privée et communications électroniques a déjà donné lieu à de vastes débats entre les autorités de contrôle et les organisations quant à sa portée, et la suppression du terme «strictement» ne fera qu'affaiblir la sécurité juridique. Il s'agit également d'une préoccupation car le groupe de travail a déjà émis des lignes directrices quant à l'interprétation du terme «strictement» dans ce contexte. Le groupe de travail a proposé la précision suivante dans son avis sur l'exemption de l'obligation de consentement pour certains cookies (WP 194):
«*un cookie est strictement nécessaire pour fournir une fonctionnalité spécifique à l'utilisateur (ou à l'abonné): si les cookies sont désactivés, la fonctionnalité ne sera pas disponible et cette fonctionnalité a été expressément demandée par l'utilisateur*

[15] Voir Tracking Preference Expression (DNT), Editor's draft, 7 mars 2016.

(ou l'abonné), en tant que partie intégrante du service de la société de l'information.»[16]

En outre, le groupe de travail a indiqué que:

«les cookies "de tiers" ne sont d'habitude pas "strictement nécessaires"» à l'utilisateur qui visite un site web, puisqu'ils se rapportent généralement à un service différent de celui qui a été "expressément demandé" par ce dernier.»[17]
Le groupe de travail a ajouté que l'utilisation de modules sociaux destinés aux personnes qui n'utilisent pas une plateforme ou un site web ne serait pas non plus considérée comme strictement nécessaire.

En outre, tandis que l'article 6, paragraphe 1, point b), du règlement proposé autorise le traitement des données de communications électroniques s'il est «nécessaire» aux fins de la sécurité, le considérant 49 du RGPD requiert que ce traitement soit «strictement nécessaire». L'omission du terme «strictement» pourrait ne pas être intentionnelle, étant donné que le considérant 21 du règlement proposé indique bel et bien que le consentement relatif à l'interférence ne doit pas être demandé lorsque cette interférence est «strictement nécessaire». Néanmoins, le règlement proposé offre l'occasion de préciser que le critère de nécessité dans le contexte de ce règlement devrait être interprété de manière restrictive pour toutes les exceptions. Le groupe de travail suggère dès lors que, pour toutes les exceptions prévues à l'article 6 et à l'article 8, paragraphe 1, du règlement proposé, le terme «strictement» soit ajouté avant le terme «nécessaire».

Par ailleurs, le règlement relatif à la vie privée et aux communications électroniques devrait explicitement autoriser l'interférence avec l'équipement aux fins de l'installation de mises à jour de sécurité. L'envoi des mises à jour de sécurité par l'internet constitue le mode privilégié d'installation de ces mises à jour sur la plupart des dispositifs des utilisateurs finaux. L'installation des mises à jour est considérée comme une interférence avec l'équipement terminal. Il existe un intérêt légitime à veiller à ce que la sécurité de ces dispositifs reste à jour. Un fournisseur de patches de sécurité devrait par conséquent être généralement en mesure d'installer les mises à jour de sécurité strictement nécessaires sans le consentement de l'utilisateur final. Il n'est toutefois pas certain que cette interférence puisse relever de l'exception à l'interdiction d'interférence fondée sur la société de l'information [article 8, paragraphe 1, point c)]. Il convient de préciser que l'installation de mises à jour de sécurité est autorisée au titre de cette exception, mais uniquement dans la mesure où i) les mises à jour de sécurité sont contenues dans un paquet discret et ne changent en rien le fonctionnement du logiciel installé sur l'équipement (y compris l'interaction avec les autres logiciels ou les paramètres choisis par l'utilisateur), ii) l'utilisateur

[16] Groupe de travail «Article 29», WP 294, avis 04/2012 sur l'exemption de l'obligation de consentement pour certains cookies, adopté le 7 juin 2012, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_fr.pdf.

[17] Ibidem.

final est informé préalablement à chaque installation de mise à jour et iii) l'utilisateur final a la possibilité de désactiver l'installation automatique de ces mises à jour.

PROSPECTION DIRECTE

L'insuffisance de la protection contre la prospection directe soulève une autre série de préoccupations.

27. Premièrement, une source de préoccupation a trait au fait que **la portée de la notion de prospection directe est trop limitée**. L'article 4, paragraphe 3, point f), du règlement proposé définit les «communications de prospection directe» comme «toute forme de publicité, tant écrite qu'orale, envoyée à un ou plusieurs utilisateurs finaux, identifiés ou identifiables, de services de communications électroniques». L'utilisation du terme «envoyé» suppose le recours à des moyens de communication électronique impliquant l'acheminement d'une communication, alors que la majeure partie des publicités sur l'internet (sur les plateformes de médias sociaux ou sur les sites web) ne donne pas lieu à un «envoi» à proprement parler. Ce point est souligné par les exemples mentionnés plus loin dans cette définition (SMS, courrier électronique) ainsi qu'au considérant 33. Tous ces exemples renvoient à des formes assez classiques de communications de prospection, et même le recours au système, plutôt traditionnel, des appels vocaux ne relève pas de cette définition. L'article et le considérant devraient être modifiés pour inclure toutes les publicités *envoyées, adressées ou présentées* à un ou plusieurs utilisateurs finaux identifiés ou identifiables. En outre, il convient de veiller à ce que les publicités comportementales (fondées sur le profil des utilisateurs) soient également considérées comme des communications de prospection directes adressées à «un ou plusieurs utilisateurs finaux identifiés ou identifiables» (étant donné que ces publicités ciblent des utilisateurs spécifiques identifiables).

    Par ailleurs, conformément à la portée actuelle de la notion de «communications de prospection directe», la protection prévue à l'article 16, paragraphe 1, serait limitée aux messages contenant du matériel publicitaire et ne protégerait pas les individus contre d'autres messages envoyés, adressés ou présentés à des fins de prospection (comme les messages de génération de leads visant à obtenir un consentement, la promotion des points de vue politiques ou des préférences électorales, la promotion d'organisations caritatives et d'autres organisations sans but lucratif ou toute autre forme de promotion générale d'une organisation). De plus, les télécopieurs sont toujours utilisés comme moyen de prospection directe, bien qu'ils ne soient pas mentionnés dans la définition. L'article 4, paragraphe 3, point f), devrait donc couvrir toute forme de publicité, prospection ou promotion, y compris pour des organisations sans but lucratif, et inclure explicitement les télécopieurs aux côtés du courrier électronique et des SMS (voir également la proposition de précision formulée au point 43 a). Enfin, le considérant 32 indique que la prospection directe couvre les messages que les partis politiques envoient afin d'assurer leur promotion. Il convient d'actualiser ce considérant pour y inclure les responsables politiques et les candidats aux élections qui assurent la promotion de leur candidature.

28. Deuxièmement, **le retrait du consentement à la prospection directe ne se fait pas sans frais, et n'est pas aussi facile que l'octroi du consentement.** La possibilité de retirer son consentement au titre du règlement proposé doit être précisée afin d'assurer la cohérence et d'améliorer la protection des destinataires. L'article 16, paragraphe 6, du règlement proposé dispose actuellement que les destinataires des communications de prospection directe doivent recevoir «les informations nécessaires [...] pour leur permettre d'exercer leur droit de retirer, de manière simple, leur consentement à continuer de recevoir des communications de prospection» (soulignement ajouté). Ce point est confirmé au considérant 34. Il ressort toutefois du considérant 70 du RGPD que les personnes concernées relevant de ce règlement doivent avoir le droit non seulement de s'opposer facilement au traitement de leurs données à des fins de prospection directe, mais aussi de le faire «sans frais». Ce terme est également utilisé à l'article 16, paragraphe 2, du règlement proposé, mais uniquement dans le contexte de l'opposition à la prospection directe sur la base de coordonnées obtenues dans le cadre de la vente d'un produit ou d'un service.

    L'article 7, paragraphe 3, du RGPD dispose qu'il doit être aussi simple de retirer que de donner son consentement et que les personnes doivent pouvoir retirer leur consentement à tout moment. En outre, dans son avis 4/2010 sur la FEDMA (WP 174), le groupe de travail a déjà reconnu l'importance d'offrir «un moyen simple, effectif, gratuit, direct et facile d'accès de se désabonner» des communications de prospection directe[18]. Cette norme en matière de retrait du consentement devrait être intégrée dans les règles applicables à la prospection directe établies par le règlement proposé. Il en va de même pour l'exigence, énoncée à l'article 7, paragraphe 3, du RGPD, selon laquelle il doit être aussi simple de retirer que de donner son consentement à tout moment.

29. Dans le même ordre d'idées, **la manière de retirer son consentement aux appels de prospection directe ou de s'opposer à ces appels devrait être précisée**. Sur la base de l'article 16, paragraphe 4, du règlement proposé, les États membres peuvent choisir, pour les appels vocaux de prospection directe, un système permettant aux utilisateurs de s'opposer à ce type d'appels. Le règlement relatif à la vie privée et aux communications électroniques devrait préciser les modalités du retrait du consentement aux appels de prospection ainsi que de l'opposition à ces appels. Le considérant 36 précise que les États membres *devraient être en mesure* de créer et/ou de maintenir des systèmes nationaux donnant à l'utilisateur la possibilité de s'opposer aux appels de prospection directe. Sur la base de cette disposition, les États membres pourraient même autoriser une situation dans laquelle un utilisateur devrait s'opposer aux appels de prospection directe auprès de chaque fournisseur de communications. Une telle mise en œuvre ne protège pas les utilisateurs contre la nuisance que

18 Groupe de travail «Article 29», WP 174, avis 4/2010 sur le code de conduite européen de la FEDMA relatif à l'exploitation de données à caractère personnel dans le cadre d'opérations de marketing direct, adopté le 13 juillet 2010, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174_fr.pdf.

constituent les communications non justifiées[19], pas plus qu'elle n'offre un mécanisme conforme au RGPD permettant de retirer son consentement de manière aisée et à tout moment. Par conséquent, le règlement devrait préciser que chaque État membre *doit* créer une liste nationale des numéros exclus. Il devrait en outre préciser que les destinataires des appels vocaux devraient se voir offrir deux possibilités pour retirer leur consentement: pour les appels futurs d'une entreprise ou d'une organisation donnée et par l'inscription, au cours de ces appels, sur une liste nationale des numéros exclus.

30. **Le fait que l'utilisation de fausses identités lors de l'envoi de communications de prospection directe ne soit pas explicitement interdite** constitue une autre source de préoccupation. Le considérant 34 indique que «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» est interdit. Toutefois, l'article 16, paragraphe 6, dispose simplement que les utilisateurs finaux doivent être informés «de l'identité de la personne morale ou physique pour le compte de laquelle la communication est transmise». Cette obligation d'informer les destinataires de l'identité de l'émetteur devrait être complétée par une interdiction claire de masquer l'adresse de contact ou d'utiliser une fausse adresse de contact à des fins de prospection directe.

31. Ce point est lié à une autre préoccupation: **l'exigence d'utilisation d'un indicatif pour les appels de prospection directe est présentée comme une solution de substitution à l'exigence d'identification d'une ligne de contact**. L'article 16, paragraphe 3, dispose que les appels de prospection directe ne sont autorisés que si l'appelant soit i) présente l'identité d'une ligne sur laquelle il peut être contacté [article 16, paragraphe 3, point a)], soit ii) utilise un code ou un indicatif spécifique indiquant qu'il s'agit d'un appel commercial [article 16, paragraphe 3, point b)]. Bien que le groupe de travail se félicite de l'obligation d'utilisation d'un indicatif établie à l'article 16, paragraphe 3, point b), il estime que cette exigence vise à répondre à un problème différent de celui auquel répond l'obligation d'identification d'une ligne de contact établie à l'article 16, paragraphe 3, point a). Tandis que l'exigence d'utilisation d'un indicatif vise à permettre au destinataire d'identifier d'emblée un appel en tant qu'appel commercial (et de prendre des mesures pour bloquer les appels de ce type), l'exigence d'identification d'une ligne de contact vise à donner au destinataire (et aux autorités de contrôle) le moyen d'identifier et de contacter la personne à l'origine de l'appel commercial. Cette question est particulièrement pertinente pour les appels automatisés, dans le cadre desquels il existe un déséquilibre important entre les possibilités pour le prospecteur d'émettre des appels importuns et les possibilités pour le destinataire d'éviter ces appels. Ces deux exigences ne doivent donc pas se substituer l'une à l'autre, mais être complémentaires l'une de l'autre.

CALENDRIER

[19] Par exemple, au Royaume-Uni, l'opérateur de télécommunications BT a enregistré le nombre record de 31 millions d'appels importuns en une semaine. Voir: http://www.bbc.com/news/business-38635921.

32. Le groupe de travail «Article 29» se réjouit que la Commission européenne reconnaisse la nécessité que le règlement proposé entre en vigueur en même temps que le RGPD en mai 2018, afin d'éviter les incohérences entre les deux actes législatifs. Toutefois, il subsiste une préoccupation à cet égard, à savoir qu'il s'agit d'un calendrier ambitieux, qui requiert également que le projet de code des communications électroniques européen soit finalisé. Le GT29 demande donc à tous les acteurs du processus législatif de s'engager à respecter le délai de mai 2018.

AUTRES PREOCCUPATIONS

La présente section examine un certain nombre de préoccupations supplémentaires.

33. Premièrement, le GT29 est préoccupé par **la suggestion selon laquelle les mesures de conservation des données non ciblées sont acceptables.** L'exposé des motifs indique que, dans le cadre du règlement proposé, les États membres restent libres de maintenir ou de créer des cadres nationaux de conservation des données qui prévoient, entre autres, des mesures de conservation ciblées (point 1.3). À la suite de l'arrêt *Tele2/Watson*[20], il est évident que les cadres de conservation des données prévoyant des mesures autres que des mesures ciblées ne sont pas autorisés par la Charte (même si elles sont soumises à des conditions strictes comme la surveillance) et que l'accès généralisé aux métadonnées doit être considéré comme une infraction à l'essence même de l'article 7, tout comme l'accès généralisé au contenu des communications électroniques (voir CJUE, Schrems, et considérant 94). Le libellé de cette phrase donne à penser que les États membres disposent d'une certaine latitude concernant les mesures de conservation des données, alors que ce n'est pas le cas. En rapport avec ce point, le règlement proposé **ne garantit pas un niveau de protection suffisant concernant les métadonnées**. Comme indiqué au point 10, le groupe de travail «Article 29» salue la reconnaissance du fait que les métadonnées peuvent révéler des informations très sensibles. Toutefois, dans le règlement proposé, les métadonnées ne bénéficient pas de la protection qui devrait découler de cette reconnaissance. Compte tenu de la sensibilité des métadonnées, en particulier, avant une analyse au titre de l'article 6, paragraphe 2, point c), une analyse d'impact relative à la protection des données devrait être effectuée (voir également le point 46).

34. Deuxièmement, **le règlement proposé élargirait de manière excessive les possibilités de conserver les données**. L'article 11 du règlement proposé renvoie à l'article 23, paragraphe 1, points a) à e), du RGPD lorsqu'il expose les finalités pour lesquelles les États membres peuvent limiter la portée des obligations et des droits prévus aux articles 5 à 8 du règlement. Le RGPD ne prévoit pas de limitations de ce type pour les catégories particulières de données, eu égard aux risques élevés pour les personnes concernées. Si l'article 15 de la directive vie privée et communications électroniques autorise une limitation similaire, les finalités sont plus restreintes. Le nouveau règlement proposé rendrait possibles de nouvelles limitations aux fins de «l'exécution de sanctions pénales, y compris la protection contre les menaces pour la

[20] ECLI:EU:C:2016:970, URL: http://curia.europa.eu/juris/celex.jsf?celex=62015CJ0203.

sécurité publique et la prévention de telles menaces» [article 23, paragraphe 1, point d), du RGPD] et «d'autres objectifs importants d'intérêt public général de l'Union ou d'un État membre, notamment un intérêt économique ou financier important de l'Union ou d'un État membre, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale» [article 23, paragraphe 1, point e), du RGPD]. Non seulement ces finalités sont nouvelles par rapport à la directive vie privée et communications électroniques actuelle, mais la dernière finalité de l'article 23, paragraphe 1, point d), et la totalité de la finalité de l'article 23, paragraphe 1, point e), sont libellées de manière extrêmement vaste. Il est par conséquent suggéré de supprimer la référence à l'article 23, paragraphe 1, points a) à e), du RGPD et de ne mentionner à la place que les finalités actuellement visées à l'article 15 de la directive vie privée et communications électroniques.

35. **L'obligation d'informer les utilisateurs des risques en matière de sécurité a une portée minimaliste**. Le groupe de travail se félicite du fait que les fournisseurs de services doivent informer les utilisateurs des risques en matière de sécurité et des mesures à prendre pour y remédier, telles que le cryptage (article 17 et considérant 37). Toutefois, l'intitulé de la disposition est libellé comme suit: «Informations sur les risques de sécurité détectés» Le fait que cet intitulé parle des risques détectés donne à penser que cette disposition ne couvre que les violations (potentielles) de la sécurité, alors que le libellé de la disposition elle-même et du considérant semble davantage viser une éducation générale des utilisateurs finaux. Par exemple, si un fournisseur de services détecte que le dispositif d'un utilisateur est infecté par un logiciel malveillant et fait désormais partie d'un réseau zombie, cette disposition semble faire obligation directe au fournisseur d'informer l'utilisateur des risques qui en découlent. Toutefois, il convient de préciser la portée de cette disposition et de ne pas la limiter à ce scénario particulier. Il convient qu'elle couvre au moins les risques en matière de sécurité détectés sur tous les équipements mis à disposition de l'utilisateur final par le fournisseur dans le cadre de l'abonnement, comme les routeurs et les dispositifs mobiles, et inclue un volet pédagogique concernant les risques liés au changement des paramètres réglés pour assurer le respect de la vie privée conformément au principe de la protection des données dès la conception.

    Le groupe de travail recommande que la portée soit élargie pour inclure les fournisseurs de logiciels permettant des communications électroniques (voir le considérant 8) et, éventuellement une nouvelle catégorie, à savoir les fournisseurs des technologies indispensables à la sécurisation des communications qui ne sont pas des fournisseurs de services (par exemple les fournisseurs des technologies de cryptage). En ce qui concerne l'extension à cette dernière catégorie, il convient de veiller à ce que cette obligation ne chevauche pas les obligations de notification des violations de la sécurité au titre d'autres instruments, tels que la directive SRI[21] et les autres instruments législatifs relatifs aux fournisseurs de certificats. Les fournisseurs de

[21] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (JO L 194 du 19.7.2016, p. 1), url: http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016L1148.

technologies appartenant à cette catégorie n'ayant généralement pas de contacts directs avec les utilisateurs finaux, il convient également d'expliquer comment ils peuvent se conformer à leur obligation en matière d'information au titre de cette disposition.

36. Le groupe de travail se félicite des dispositions des articles 2 et 13 qui s'appliqueront aux services de communications interpersonnelles fondés sur la numérotation. Toutefois, on ne voit pas a priori pourquoi un **niveau similaire de protection de la vie privée ne devrait pas aussi s'appliquer dans le cas des services de communication par contournement (OTT) équivalents du point de vue fonctionnel.**

37. Le groupe de travail est également préoccupé par le **manque de clarté concernant le consentement granulaire pour les recherches inverses dans les annuaires**. L'article 15, paragraphe 2, du règlement proposé exige que les fournisseurs obtiennent le consentement des utilisateurs finaux avant d'activer les fonctions de recherche en relation avec les données (voir également le considérant 31). Le groupe de travail se félicite de l'harmonisation de l'exigence de consentement en ce qui concerne l'inclusion dans les annuaires, mais regrette le manque de granularité quant aux différents types de recherches. La directive vie privée et communications électroniques actuelle autorise les États membres à exiger un consentement distinct pour la recherche inverse, conformément à l'article 12, paragraphe 3. Aux termes de cet article, les États membres «*peuvent demander que le consentement des abonnés soit également requis pour toute finalité d'annuaire public autre que la simple recherche des coordonnées d'une personne sur la base de son nom et, au besoin, d'un nombre limité d'autres paramètres*». Sur la base de cette disposition, dans de nombreux États membres, un consentement distinct est requis pour les fonctions de recherche inverse, étant donné les niveaux différents d'identifiabilité et, partant, d'intrusion, des deux fonctions.

38. Sur un plan plus formel, **le niveau des amendes n'est pas harmonisé pour toutes les infractions au règlement**. Le règlement proposé prévoit que les États membres fixent les règles concernant les amendes pour les infractions à son article 23, paragraphe 4, à son article 23, paragraphe 6, et à son article 24. Il serait plus cohérent de régler cette question dans le règlement relatif à la vie privée et aux communications électroniques lui-même.

39. Enfin, **le règlement proposé repose sur des définitions susceptibles de devenir des «cibles mouvantes»**. Pour un certain nombre de ses notions clés, le règlement proposé renvoie à un autre instrument juridique actuellement à l'état de projet: le code des communications électroniques européen proposé [voir par exemple l'article 4, paragraphe 1, point b)]. La définition de l'«utilisateur final», qui inclut actuellement les personnes physiques et morales, et les définitions des «services de communications électroniques» et des «services de communications interpersonnelles», qui sont visées à l'article 4, paragraphe 1, point b), et, dans le cas des services de communications interpersonnelles, précisées à l'article 4,

paragraphe 2, pour inclure des types de services spécifiquement exclus du code des communications électroniques européen[22], constituent deux exemples importants à cet égard. Le présent avis se fonde sur les définitions dans leur libellé actuel; il est toutefois assez probable que le code des communications électroniques européen proposé et/ou ses notions clés seront modifiés, ce qui aurait des répercussions immédiates sur le règlement relatif à la vie privée et aux communications électroniques également. Idéalement, tous les termes issus du code des communications électroniques européen devraient être définis de manière indépendante dans le règlement relatif à la vie privée et aux communications électroniques, ou, à tout le moins, le règlement proposé devrait comporter des précisions lorsque la définition de certains termes s'écarte de celle contenue dans le code des communications électroniques européen (par exemple l'inclusion susmentionnée des «services auxiliaires» dans la définition du «service de communications interpersonnelles»). Toutefois, si cela ne devait pas être possible, le groupe de travail aimerait suggérer à toutes les parties impliquées dans le processus législatif de veiller à ce que le règlement proposé et le code des communications électroniques européen soient examinés et soumis au vote simultanément, afin que les parties prenantes puissent évaluer correctement le champ d'application et les implications des nouveaux instruments.

5. SUGGESTIONS DE PRÉCISIONS POUR ASSURER LA SÉCURITÉ JURIDIQUE

Outre les points examinés ci-dessus, le groupe de travail souhaite également mettre en évidence certaines dispositions du règlement proposé qui gagneraient à être précisées. Ces précisions sont jugées nécessaires pour assurer à tous les acteurs concernés une plus grande sécurité juridique quant au fait que le règlement relatif à la vie privée et aux communications électroniques sera interprété et appliqué de manière uniforme dans toute l'Union européenne.

PRECISIONS CONCERNANT LE CHAMP D'APPLICATION

40. En ce qui concerne le champ d'application du règlement proposé, le GT29 suggère les précisions ci-après.

    a. **Le terme «utilisateur final» devrait inclure tous les utilisateurs individuels**. L'article 2, point 14), du code des communications électroniques européen définit l'«utilisateur final» comme un utilisateur qui ne fournit pas de réseaux de communication publics ou de services de communications électroniques accessibles au public. Il convient de préciser que les particuliers

[22] Par exemple, l'article 4, paragraphe 2, du règlement proposé dispose que les services de communications interpersonnelles comprennent «les services qui rendent possible une communication interpersonnelle et interactive uniquement en tant que fonction mineure accessoire intrinsèquement liée à un autre service», tandis que l'article 2, paragraphe 5, du code des communications électroniques européen exclut explicitement ce type de services de la définition [le code des communications électroniques européen inclut les «services de communications interpersonnelles» dans la catégorie plus vaste des «services de communications électroniques» à l'article 2, point 4)].

qui contribuent aux réseaux, par exemple au maillage des réseaux au moyen de leur routeur Wi-Fi, ne sont pas exclus du champ d'application de la protection prévue par le règlement proposé.

b. **Il convient de préciser que le champ d'application territorial couvre tous les utilisateurs finaux dans l'Union**. L'article 3, paragraphe 1, point a), dispose que le règlement proposé s'applique à la fourniture de services de communications électroniques aux utilisateurs finaux «dans l'Union», tandis que l'article 3, paragraphe 1, point c), dispose qu'il s'applique à la protection des informations liées aux équipements terminaux des utilisateurs finaux «situés dans l'Union» (soulignement ajouté). Ces dispositions varient selon les versions linguistiques. La version allemande ne fait pas cette distinction, à l'inverse d'autres, comme les versions anglaise, espagnole et néerlandaise. Il ressort clairement du considérant 9 que le champ d'application territorial se veut large, que les services soient ou non fournis depuis l'extérieur de l'Union ou que le traitement ait lieu ou non dans l'Union. Il est par conséquent suggéré de supprimer le terme «situés» à l'article 3, paragraphe 1, point c), afin de souligner ce large champ d'application.

c. **Le règlement proposé semble uniquement protéger la confidentialité des communications pendant leur *transfert*, et non une fois qu'elles sont *stockées***. L'approche actuelle du règlement proposé se concentre sur la protection de la transmission des communications. Par exemple, le considérant 15 indique que l'interdiction de l'interception des données de communications devrait s'appliquer durant leur acheminement, c'est-à-dire jusqu'à la réception du contenu de la communication électronique par le destinataire. L'étendue de cette protection se fonde sur un cadre conceptuel des communications qui est dépassé. La plupart des données de communications restent stockées auprès des fournisseurs de services, même après réception par le destinataire. Il convient de veiller à ce que la confidentialité de ces données reste protégée. En outre, dans le cas des communications entre abonnés des mêmes services en nuage (par exemple un fournisseur de courrier électronique), l'acheminement de données est souvent très limité: l'envoi d'un courrier électronique implique pour l'essentiel l'inscription de celui-ci dans la base de données du fournisseur, plutôt que l'envoi réel de données de communication entre deux parties. L'argument selon lequel cette situation serait déjà couverte par le RGPD n'est pas convaincant: tout l'objet du règlement proposé consiste à protéger l'ensemble des communications confidentielles, indépendamment des moyens techniques sur lesquels elles reposent. Il est possible qu'il s'agisse d'une simple erreur de rédaction, étant donné que l'interdiction établie à l'article 5 concerne le «stockage» et le «traitement».

d. **Tous les points d'accès internet sans fil (*hotspots*) devraient relever du champ d'application**. Étant donné que l'utilisation des points d'accès sans fil est courante, il ne devrait, en toute logique, y avoir aucun doute quant au fait que la confidentialité des communications acheminées via ces points d'accès est protégée. La tentative de préciser ce point contenue dans le règlement n'atteint pas son objectif, étant donné que le champ d'application n'est étendu qu'aux réseaux fournis «à un groupe indéfini d'utilisateurs

finaux» (considérant 13). Les termes «groupe indéfini d'utilisateurs finaux» et «groupe fermé d'utilisateurs finaux» doivent être définis. Il convient en particulier de préciser que les réseaux sans fil sécurisés (c'est-à-dire nécessitant un mot de passe) relèvent également du champ d'application du règlement si ce mot de passe est fourni à un groupe théoriquement indéfini d'utilisateurs dont l'identité ne peut être déterminée à l'avance (par exemple les clients d'un café, les visiteurs d'un aéroport). Le principe sous-jacent à cet égard est que, conformément à l'avis précédent du GT29 sur la révision de la directive vie privée et communications électroniques, seuls peuvent être exonérés de l'instrument relatif à la vie privée et aux communications électroniques, les services qui se déroulent dans un cadre officiel ou professionnel uniquement à des fins professionnelles ou officielles, ou les communications techniques entre des organismes non publics et des organismes publics ayant pour seul objet de contrôler des processus de travail ou des processus opérationnels, ainsi que l'utilisation de services à des fins exclusivement domestiques (p. 8).

e. **Les données collectées dans le contexte de la fourniture de services de radiotélévision numérique devraient être couvertes par le règlement proposé.** Compte tenu de la nature sensible du comportement des téléspectateurs, qui révèle les intérêts et caractéristiques de ces derniers, le règlement relatif à la vie privée et aux communications électroniques devrait préciser (peut-être au moyen d'un considérant) que l'exclusion des services «consistant à fournir des contenus à l'aide de réseaux [...] de communications électroniques» de la définition du «service de communications électroniques» ne signifie pas que les prestataires de services offrant à la fois des services de communications électroniques et des services de contenu ne relèvent pas du champ d'application des dispositions du règlement relatif à la vie privée et aux communications électroniques qui ciblent les fournisseurs de services de communications électroniques. Ce point est particulièrement pertinent dans la mesure où la prestation de services «consistant à fournir des contenus à l'aide de réseaux [...] de communications électroniques» est exclue de la définition du «service de communications électroniques» établie par la proposition de code des communications électroniques européen (article 2, paragraphe 4).

f. **Les données de communications sont, de manière générale, des données à caractère personnel**. Il est indiqué, au considérant 4, que les données de communications peuvent comporter des données à caractère personnel. Toutefois, la plupart des données de communications sont des données à caractère personnel[23] et, pour une grande partie d'entre elles, des données de nature plutôt intime et sensible, de sorte qu'il convient de modifier ce considérant pour préciser que ces données sont, de manière générale, des données à caractère personnel.

[23] Voir, par exemple, les arrêts de la Cour de justice de l'Union européenne du 6 novembre 2003 dans l'affaire C-101/01, point 24 (concernant un numéro de téléphone), du 19 octobre 2016 dans l'affaire C-582/14, *Breyer*, point 49 (concernant les adresses IP dynamiques) et du 8 avril 2014 dans les affaires jointes C-239/12 et C-594/12, *Digital Rights Ireland*, points 26 et 27 (concernant la sensibilité des métadonnées).

g. **Les communications confidentielles incluent les messages publiés sur des plateformes**. Le considérant 1 indique que le principe de confidentialité s'applique «aux moyens de communication actuels et futurs» et poursuit avec une liste d'exemples de ces moyens, dont «la messagerie personnelle fournie par les réseaux sociaux». L'objectif est probablement d'inclure les messages privés entre utilisateurs d'un réseau social (comme Facebook ou Twitter) ou les messages publiés sur un fil d'actualité (*timeline*) qui sont accessibles à un nombre défini de personnes, mais le libellé n'est pas suffisamment clair.

h. **Manière dont le règlement relatif à la vie privée et aux communications électroniques s'applique aux interactions de machine à machine.** Comme indiqué au point 9, le groupe de travail se félicite de l'extension de la protection aux interactions de machine à machine. Toutefois, cette extension n'est mentionnée qu'au considérant 12, et non dans un article correspondant. Cette protection est souhaitable, étant donné que ces communications contiennent souvent des informations protégées au titre des droits liés au respect de la vie privée. Néanmoins, il convient d'exempter une catégorie limitée de communications s'effectuant exclusivement de machine à machine lorsqu'elles n'ont pas d'incidence sur le respect de la vie privée ni sur la confidentialité des communications; il s'agit par exemple des cas dans lesquels les communications de ce type font partie de l'exécution d'un protocole de transmission entre éléments d'un réseau (par exemple des serveurs ou des commutateurs) visant exclusivement à permettre aux différents éléments de s'informer de leur statut d'activité respectif.

   Il existe un domaine particulier dans lequel l'application du règlement relatif à la vie privée et aux communications électroniques doit être précisée: celui des systèmes de transport intelligents. Dans ces systèmes, les véhicules devraient transmettre en permanence, par voie hertzienne, des données contenant un identifiant unique. Sans la protection supplémentaire prévue par le règlement relatif à la vie privée et aux communications électroniques, cela pourrait déboucher sur un suivi continu des habitudes de conduite, des trajets et de la vitesse des conducteurs. L'article 2, point 1), du code des communications électroniques européen contient toutefois une nouvelle définition, élargie, des réseaux de communications électroniques. Ceux-ci incluent les systèmes de transmission qui ne disposent pas d'une capacité d'administration centralisée et permettent l'acheminement de signaux par voie hertzienne. Le considérant 14 du règlement relatif à la vie privée et aux communications électroniques précise que ces données constituent des données de communications électroniques. En application de l'article 5 du règlement proposé, tout type d'interception, de surveillance ou de stockage de ces données de communications est interdit, à moins qu'une des exceptions ne s'applique. Pourtant, le traitement de ces données permettant à des objets tels que les voitures et dispositifs sans conducteur de s'avertir mutuellement de leur proximité ou d'autres risques présente un intérêt. La question se pose alors de savoir quelle exception devrait s'appliquer dans ce cas. Le consentement des utilisateurs finaux n'est pas une exception envisageable car il pourrait devenir nécessaire de pouvoir traiter ces données en permanence. Il convient donc que les fournisseurs puissent se fonder sur une exception

spécifique permettant à des objets tels que les voitures et dispositifs sans conducteur de s'avertir mutuellement de leur proximité ou d'autres risques.

PRECISION CONCERNANT LA NOTION DE CONSENTEMENT ET SON APPLICATION

41. En ce qui concerne la notion de consentement et son application dans le règlement proposé, le GT29 propose les précisions ci-après.
    a. **Application de la notion de consentement dans le contexte de personnes morales.** Le considérant 3 indique que le règlement devrait garantir que les dispositions du RGPD s'appliquent également aux utilisateurs finaux qui sont des personnes morales. Cela comprend, selon le même considérant, la définition du consentement en vertu du RGPD (voir également le considérant 18). Comme indiqué au point 13, le groupe de travail se félicite de l'inclusion explicite des personnes morales dans le champ d'application du règlement. L'application pratique de ce principe n'est toutefois pas claire. La définition du consentement au titre du RGPD exige que ce consentement soit «éclairé» et que la manifestation de la volonté de la personne concernée se fasse «par une déclaration ou par un acte positif clair» [article 4, point 11), du RGPD]. Il convient de préciser quand une personne morale peut effectivement être considérée comme étant «éclairée» et quand il y a une telle manifestation de volonté par une personne morale.
    b. Dans ce contexte, il est utile de souligner que, dans la plupart des situations, l'employeur ne peut pas donner son consentement au nom de ses employés, étant donné que, lorsqu'un employeur exige le consentement d'un employé, et que, compte tenu du déséquilibre des pouvoirs, l'absence de consentement peut entraîner un préjudice réel ou potentiel, le consentement n'est pas valable dans la mesure où il n'est pas donné librement[24]. En ce qui concerne les **sociétés mettant des dispositifs ou équipements à la disposition d'individus, le règlement proposé ne contient pas d'exception (appropriée)** à l'interdiction d'interférence. On songera notamment au cas dans lequel l'employeur souhaite mettre à jour un téléphone fourni par la société. Ou encore au cas dans lequel un employeur offre des voitures en crédit-bail à ses employés et, pour des raisons administratives, autorise un tiers à collecter des données de localisation au moyen de l'unité embarquée des véhicules. Dans les deux cas, l'employeur a un intérêt à interférer avec ces dispositifs.
       Cette interférence ne peut être considérée comme nécessaire pour fournir un service de la société de l'information [article 8, paragraphe 1, point c)] ou nécessaire pour mesurer des résultats d'audience sur le web [article 8, paragraphe 1, point d)]. Pour remédier à cette situation, il serait possible de définir une nouvelle exception, couvrant les situations dans lesquelles i) l'employeur met certains équipements à disposition dans le cadre d'une

[24] Voir l'avis 15/2011 sur la définition du consentement (WP 187), l'avis 8/2001 sur le traitement des données à caractère personnel dans le contexte professionnel (WP 48) et le nouvel avis sur le traitement des données au travail (adopté en même temps que le présent avis).

relation d'emploi, ii) l'employé est l'utilisateur de ces équipements et iii) l'interférence est strictement nécessaire à l'utilisation des équipements par l'employé (ce qui suppose l'application des principes de proportionnalité et de subsidiarité en ce qui concerne la collecte des données). Ce n'est que sous réserve que ces conditions soient remplies qu'il devrait être possible pour l'employeur d'interférer avec le dispositif de l'utilisateur final.

c. **Amélioration des moyens visant à mettre fin au renvoi automatique des appels**. L'article 14 fournit un moyen important permettant aux utilisateurs finaux de mettre fin au renvoi automatique des appels par un tiers. Cette protection pourrait être renforcée si l'on exigeait le consentement de l'utilisateur final avant de démarrer le renvoi automatique des appels.

CLARIFICATIONS CONCERNANT LES DONNEES DE LOCALISATION ET LES AUTRES METADONNEES

42. Le groupe de travail propose de préciser les aspects ci-après en ce qui concerne les données de localisation et autres métadonnées.
    a. La signification de l'expression **«données de localisation qui sont générées dans un contexte autre que celui de la fourniture de services de communications électroniques» figurant au considérant 17 devrait être précisée**. Il est difficile de déterminer si cette expression concerne les données de localisation collectées, par exemple, par les applications utilisant les données de la fonction GPS des dispositifs intelligents et/ou les données de localisation générées sur la base des routeurs Wi-Fi situés à proximité et/ou les données de localisation collectées au moyen des assistants de navigation embarqués et/ou les données de localisation générées d'autres manières. Ce manque de clarté est source d'insécurité juridique quant à la portée de l'obligation. En tout état de cause, les données de localisation du dispositif terminal d'une personne physique constituent des données à caractère personnel, dont le traitement est donc soumis aux obligations découlant du RGPD.
    b. Il convient de préciser que **la plupart des traitements légitimes de données de localisation et autres métadonnées <u>ne</u> requièrent <u>pas</u> d'identifiant unique**. Le considérant 17 cite les cartes de densité de clics comme exemple d'utilisation commerciale de métadonnées de communications électroniques par des fournisseurs de services de communications électroniques. Toutefois, pour créer une carte de densité de clics de base, aucun identifiant unique n'est nécessaire, un simple comptage statistique suffit. Un autre exemple mentionné dans ce considérant, l'usage des infrastructures existantes et de la pression que celles-ci subissent, peut également être déterminé au moyen de certains points de mesures, par exemple en créant des statistiques agrégées sur l'utilisation des tours de trafic pour donner une indication de la pression à un endroit et à un moment donnés, sans qu'il soit nécessaire de connaître exactement l'identité des personnes connectées.

       En outre, le considérant mentionne l'exemple de l'affichage des mouvements de trafic dans certaines directions au cours d'une période de temps

déterminée, pour lequel un identifiant serait nécessaire afin de relier les positions des individus à des intervalles de temps donnés. Avec cet exemple, le considérant semble légitimer le traitement ultérieur de ces données à l'appui de l'analyse des «mégadonnées». La seule condition à laquelle le règlement proposé subordonne ce type de traitement est l'obligation de procéder à une analyse d'impact relative à la protection des données lorsque le traitement *est susceptible de présenter un risque élevé pour les droits et libertés de personnes physiques*. Cette condition est insuffisante. Elle est également contraire à l'obligation établie à l'article 6, en vertu duquel ce type de traitement ne peut être réalisé qu'avec le consentement des utilisateurs, et uniquement si l'anonymisation des données, c'est-à-dire l'utilisation de données ne contenant aucun identifiant unique, n'est pas possible. Il arrive souvent que les utilisateurs ne puissent pas refuser la collecte de leurs données de géolocalisation par les fournisseurs de services de communications électroniques, lorsque cette collecte est techniquement nécessaire à l'acheminement des communications vers l'utilisateur ou lorsque le traitement de ces données est nécessaire à la fourniture du service (par exemple de navigation) demandé. Dans ses avis antérieurs, le groupe de travail a conclu que les données de localisation provenant des dispositifs intelligents constituent des données à caractère personnel de nature sensible et que les avantages liés à l'analyse de ces données ne priment pas sur les droits des utilisateurs à la protection de la confidentialité de leurs métadonnées de communication, ni sur les droits généraux à la protection des données établis par le RGPD. Par conséquent, le considérant doit au minimum préciser que les fournisseurs sont tenus de se conformer aux obligations établies à l'article 25 du RGPD en cas de traitement ultérieur des données de localisation ou d'autres métadonnées. Il s'ensuit que les mesures suivantes au moins doivent être prises:

i) l'utilisation de pseudonymes temporaires;

ii) la suppression de tout tableau permettant d'établir une correspondance entre ces pseudonymes et les données d'identification originales;

iii) l'agrégation des données à un niveau où les utilisateurs individuels ne peuvent plus être identifiés par leur parcours spécifique et

iv) la suppression des observations extrêmes au regard desquelles l'identification resterait possible (toutes ces mesures doivent être appliquées ensemble).

Enfin, le règlement relatif à la vie privée et aux communications électroniques doit contraindre les parties participant au traitement des données de localisation et autres métadonnées à rendre publiques leurs méthodes d'anonymisation et d'agrégation, sans préjudice du secret protégé par la loi. Cela permettrait aux autorités de contrôle et au grand public de vérifier facilement si la méthode choisie est adéquate.

PRECISIONS CONCERNANT LES COMMUNICATIONS NON SOLLICITEES

43. Le groupe de travail propose de préciser les aspects ci-après en ce qui concerne les communications non sollicitées.

    a. **Libellé de l'interdiction de prospection directe sans consentement**. L'article 16, paragraphe 1, du règlement proposé dispose actuellement que les services de communications électroniques «peuvent» être utilisés pour l'envoi de communications de prospection directe (moyennant consentement), mais n'interdit pas explicitement l'envoi (ou la présentation) de telles communications sans consentement. Cette approche contraste avec celle retenue dans les autres dispositions, qui formulent une interdiction, suivie par certaines exceptions spécifiques. Le libellé actuel suggère une approche plus souple (ce qui n'est sans doute pas volontaire). Le groupe de travail propose un libellé légèrement modifié de l'article 13, paragraphe 1, de la directive vie privée et communications électroniques: «L'utilisation, par des personnes physiques ou morales, des services de communications électroniques, y compris les appels vocaux, les systèmes automatisés d'appel et de communication sans intervention humaine (y compris les systèmes semi-automatisés qui connectent la personne appelée à un individu), les télécopieurs ou le courrier électronique, aux fins de la présentation de communications de prospection directe aux utilisateurs finaux ne peut être autorisée que si elle vise des utilisateurs finaux ayant donné leur consentement préalable.»

    b. **Portée des dispositions relatives aux communications et appels de prospection adressés à des contacts existants.** L'article 16, paragraphe 2, dispose que, lorsqu'une personne physique ou morale obtient d'un client existant ses coordonnées électroniques, ladite personne physique ou morale peut exploiter ces coordonnées électroniques à des fins de prospection directe pour ses propres produits ou services uniquement si le client se voit donner clairement la faculté de s'opposer, sans frais et de manière simple, à une telle exploitation, au moment où les coordonnées sont recueillies et lors de l'envoi de chaque message. Cette disposition est actuellement limitée aux contacts commerciaux obtenus «dans le cadre de la vente d'un produit ou d'un service» et à des fins de prospection commerciale pour des produits ou services analogues que la personne physique ou morale fournit elle-même. Étant donné que les dispositions relatives à la prospection directe s'appliquent également aux activités promotionnelles non commerciales (par exemple des organisations caritatives et des partis politiques), il convient de modifier cette disposition afin qu'elle s'applique également aux organisations non commerciales qui contactent d'anciens soutiens pour promouvoir des objectifs et idéaux analogues qu'elles-mêmes défendent, et le même droit d'opposition devrait s'appliquer aux appels de prospection directe. En outre, une période de validité maximale devrait être fixée pour les «clients existants» dans le contexte des communications électroniques à des fins commerciales, caritatives ou politiques, et cette période de validité maximale devrait également s'appliquer aux appels de prospection directe. Lorsque les États membres ont opté pour un système d'opposition aux appels vocaux de prospection, la présence d'une relation de type «client existant» supplante l'inscription sur une liste de numéros exclus. Dans ces circonstances, les

utilisateurs finaux n'ont pas la possibilité effective d'éviter les appels importuns de la part de sociétés ou d'organisations avec lesquelles ils ont été en relation par le passé, mais ne souhaitent plus avoir de contacts. Par conséquent, en règle générale, le règlement devrait préciser une durée de validité pour cette exception concernant les «clients existants», par exemple un an ou deux, selon les attentes légitimes des utilisateurs finaux concernés.

c. **Application des règles relatives à la prospection directe aux personnes morales**. L'article 16, paragraphe 5, du règlement proposé dispose que les États membres doivent veiller à ce que l'intérêt légitime des utilisateurs finaux qui sont des personnes morales soit suffisamment protégé à l'égard des communications non sollicitées. L'article 13, paragraphe 5, de la directive vie privée et communications électroniques actuelle fait référence aux intérêts légitimes des abonnés autres que les personnes physiques. Les implications de ce changement de libellé ne sont pas claires. Il convient de préciser, dans les considérants, que cette modification ne témoigne pas d'une intention d'abaisser le niveau de la protection. À cet égard, l'interdiction de prospection directe sans consentement concerne les «utilisateurs finaux qui sont des personnes physiques ayant donné leur consentement» (soulignement ajouté). Il convient de préciser que les personnes physiques *travaillant pour* des personnes morales sont également couvertes. Par ailleurs, le consentement n'est pas nécessaire pour contacter des personnes morales au moyen de coordonnées génériques qu'elles ont rendues publiques à cet effet (par exemple «info@nomdelasociete.eu»).

d. **Application des règles relatives à la prospection directe aux personnes agissant en qualité de représentants (politiques).** Dans son libellé existant, l'article 16 pourrait empêcher certaines communications envoyées à des représentants élus soulignant des préoccupations ou intérêts commerciaux. Il convient de préciser que le règlement n'empêche pas ces communications.

PRECISIONS CONCERNANT L'APPLICATION DES INSTRUMENTS LIES AUX DROITS FONDAMENTAUX

44. **L'application de la Charte et de la CEDH aux législations nationales en matière de conservation des données** devrait être davantage précisée. Le considérant 26 indique que toutes les mesures adoptées par les États membres pour assurer la sauvegarde des intérêts publics, comme les mesures d'interception légale, doivent être conformes à la Charte (en plus de la CEDH). Cette indication est souhaitable, étant donné qu'elle est conforme au raisonnement de l'affaire *Tele2/Watson*, selon lequel toute exception nationale aux protections offertes par la législation de l'Union en matière de traitement des données est subordonnée au respect de la Charte (et les infractions découlant des législations nationales peuvent donc être portées devant la Cour de justice de l'Union européenne). L'article 11 du règlement proposé dispose toutefois simplement que les limitations de la portée des articles 5 à 8 doivent respecter l'essence des libertés et droits fondamentaux et constituer une mesure nécessaire et proportionnée. Une référence explicite à la Charte et à la CEDH devrait également figurer ici.

45. **La confidentialité des communications est également protégée en vertu de l'article 8 de la CEDH**. Il est indiqué, au point 1.1 de l'exposé des motifs et au considérant 1, que le règlement proposé transpose l'article 7 de la Charte. Cette indication est répétée au considérant 19. Le droit fondamental à la confidentialité des communications n'est toutefois pas uniquement protégé par cette disposition, mais également par l'article 8 de la CEDH. L'inclusion d'une référence explicite à cet article dans un des articles du règlement proposé permettrait de confirmer davantage que toute jurisprudence de la Cour européenne des droits de l'homme en la matière devra également être prise en compte lors de l'évaluation du règlement (définitif). Cette référence figure d'ailleurs déjà aux considérants 20 (concernant les équipements terminaux) et 26 (concernant l'interception légale), et elle est en outre étayée par les considérations du point 2.1 de l'exposé des motifs (concernant la relation entre la Charte et la CEDH pour ce qui est des personnes morales), mais elle n'apparaît dans aucun des articles pertinents, comme l'article 11, paragraphe 1.

AUTRES PRECISIONS

46. Il convient de préciser que **les obligations au titre du RGPD, par exemple en ce qui concerne le système de notification des violations de données et les analyses d'impact relatives à la protection des données, restent applicables** lorsque les parties traitent des données à caractère personnel dans le contexte des données de communications électroniques. Étant donné qu'il est indiqué, au considérant 5, que le règlement proposé constitue une *lex specialis* par rapport au RGPD et que le traitement des données de communications électroniques ne devrait être permis que conformément au règlement proposé, on peut se demander si certaines obligations établies par le RGPD s'appliquent également dans le cadre du règlement proposé. Ce qui précède vaut en particulier lorsque le règlement proposé pourrait être interprété comme prévoyant une certaine obligation alors que le RGPD couvre également la question considérée. On peut citer les exemples suivants:
    i) le règlement proposé impose une certaine notification des risques pour la sécurité «détectés» (article 17) (voir également le point 35), mais le RGPD prévoit un système de notification des violations de données (articles 33 et 34);
    ii) le règlement proposé dispose que la réalisation d'une analyse d'impact relative à la protection des données et la consultation de l'autorité de contrôle conformément au RGPD sont obligatoires dans certaines circonstances [considérants 17 et 19 et article 6, paragraphe 3, point b)], alors que le RGPD détermine déjà quand une telle analyse doit être réalisée et quand une consultation est requise (articles 35 et 36); et
    iii) il n'est pas indiqué clairement que, si l'on satisfait aux conditions nécessaires pour une exception à l'interdiction de traitement au titre de l'article 5 du règlement proposé, l'on doit toujours respecter l'ensemble des obligations pertinentes au titre du RGPD dans la mesure où celui-ci concerne le traitement des données à caractère personnel et tout autre traitement au titre du RGPD est interdit. Il convient de préciser que le critère de compatibilité énoncé à l'article 6, paragraphe 4, du RGPD ne s'applique donc pas;

iv) le règlement proposé relatif à la vie privée et aux communications électroniques ne prévoit pas de mécanismes de certification semblables à ceux prévus aux articles 42 et 43 du RGPD. Étant donné que le champ d'application de l'article 42 du RGPD est, stricto sensu, limité à la mise en place de mécanismes de certification en matière de protection des données ainsi que de labels et de marques en la matière, aux fins de démontrer la conformité avec le RGPD, il convient d'examiner si une disposition comparable ne devrait pas être introduite pour permettre la certification des opérations de traitement, des normes, des produits et des services au regard de leur conformité avec le règlement relatif à la vie privée et aux communications électroniques.

Afin que ce manque de clarté ne soit pas utilisé comme argument pour abaisser le niveau de protection au titre du règlement proposé, il convient d'indiquer clairement que, dans tous ces cas, les responsables du traitement doivent également se conformer au RGPD.

47. Par ailleurs, il convient de préciser que **l'exigence relative au retrait du consentement s'applique également dans le contexte de l'interférence avec l'équipement terminal**. L'article 8, paragraphe 1, point b), du règlement proposé prévoit la possibilité d'interférer avec l'équipement terminal de l'utilisateur final sous réserve du consentement de ce dernier. L'article 9, paragraphe 3, exige que les utilisateurs finaux aient la possibilité de retirer leur consentement à tout moment, mais cette disposition ne s'applique qu'au consentement à l'analyse des métadonnées et du contenu. Il convient de préciser que cette obligation s'étend également à l'interférence avec l'équipement terminal.

48. Dans le même ordre d'idées, il convient de préciser que **le rappel de la possibilité de retirer son consentement s'applique également au consentement donné par l'intermédiaire des paramètres du navigateur.** L'article 9, paragraphe 3, exige que la possibilité de retirer leur consentement soit rappelée aux utilisateurs finaux à intervalles réguliers de six mois. Bien que le groupe de travail estime que les paramètres généraux (c'est-à-dire non fondés sur des contrôles granulaires spécifiques) des navigateurs et autres logiciels, y compris les systèmes d'exploitation, applications et interfaces logicielles pour les dispositifs connectés à l'internet des objets, ne peuvent constituer une possibilité valable d'octroi du consentement, ces paramètres n'étant pas appropriés pour que l'utilisateur puisse donner son consentement spécifique dans des situations spécifiques (voir le point 24), les paramètres par défaut doivent être favorables à l'utilisateur (voir le point 19). *Si* cette possibilité est maintenue dans le règlement proposé, les paramètres doivent être suffisamment granulaires pour contrôler tous les traitements de données auxquels l'utilisateur consent et couvrir chaque fonction de l'équipement qui pourrait donner lieu à un traitement de données. En outre, il devrait être rappelé à l'utilisateur au moins à intervalles réguliers (de six mois) qu'il a la possibilité de retirer son consentement.

49. Le groupe de travail se félicite que le règlement proposé exige que les logiciels déjà mis sur le marché informent l'utilisateur final des paramètres de confidentialité qu'il a la possibilité d'activer (article 10). **Toutefois, on ne voit pas bien comment cette**

exigence peut être effectivement appliquée aux anciens produits et autres qui ne sont plus pris en charge. En outre, il convient de préciser comment cette obligation s'appliquera aux logiciels libres qui sont développés de manière ouverte et décentralisée.

50. Il y a lieu de préciser que **le fait d'offrir la possibilité de bloquer les cookies (de tiers) en vertu de l'article 10 du règlement proposé l'emporte sur l'exception relative à la mesure des résultats d'audience sur le web** prévue à l'article 8, paragraphe 1, point d). En d'autres termes, même si un site internet recourt à l'analyse pour la mesure des résultats d'audience sur le web au titre de l'article 8, paragraphe 1, point d), les utilisateurs devraient toujours avoir le droit de bloquer ces technologies de suivi dans leur navigateur.

51. La **définition des systèmes de communication et d'appel (semi-)automatisés devrait être précisée**. La définition de ce terme figurant à l'article 4, paragraphe 3, point h), du règlement proposé contient une référence au terme lui-même dans la seconde partie de la phrase («notamment des appels effectués à l'aide de systèmes de communication et d'appel automatisés qui relient la personne appelée à une personne physique»). Il est proposé de supprimer cette partie de phrase de la définition et de modifier la définition figurant à l'article 4, paragraphe 3, point g), afin d'y inclure les appels effectués à l'aide de systèmes de communication semi-automatisés, par exemple les composeurs automatiques de numéros, qui relient la personne appelée à une personne physique.

52. L'expression **«informations concernant l'abonnement au service» doit être précisée**. Le considérant 14 indique que 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» des métadonnées de communications électroniques. On ne voit pas précisément ce que signifie cette expression.

53. Il convient de préciser **l'applicabilité des mécanismes de contrôle de la cohérence et de coopération**. Le considérant 38 indique que le règlement proposé repose sur le mécanisme de contrôle de la cohérence du RGPD. En outre, l'article 18, paragraphe 1, dispose que les chapitres VI et VII du RGPD s'appliquent par analogie. L'article 19 dispose par ailleurs que le comité européen de la protection des données s'acquitte des missions prévues à l'article 70 du RGPD. Bien que l'application de ces dispositions soit relativement claire, il ne peut être exclu que certaines questions d'interprétation se posent concernant les notions clés des mécanismes de contrôle de la cohérence et de coopération au titre du RGPD. Par exemple, le mécanisme de l'autorité de contrôle chef de file s'applique en cas de «traitement transfrontalier» (article 56, paragraphe 1, du RGPD): la manière dont cette notion s'applique dans le cas de l'interférence avec les équipements terminaux ou de l'analyse du contenu ou des métadonnées dans le cadre du règlement proposé n'est pas claire. Il est donc souhaitable de préciser l'application de ces notions clés dans un considérant et de souligner que toute question qui demeurerait au sujet de l'applicabilité de ces chapitres du RGPD dans le contexte du règlement proposé sera résolue par une interprétation des dispositions de ces chapitres conforme à leur intention. En outre, il

est utile de préciser que l'article 70 s'applique par analogie au comité européen de la protection des données dans le contexte du règlement proposé (ce point fait actuellement défaut dans le considérant).

* * *