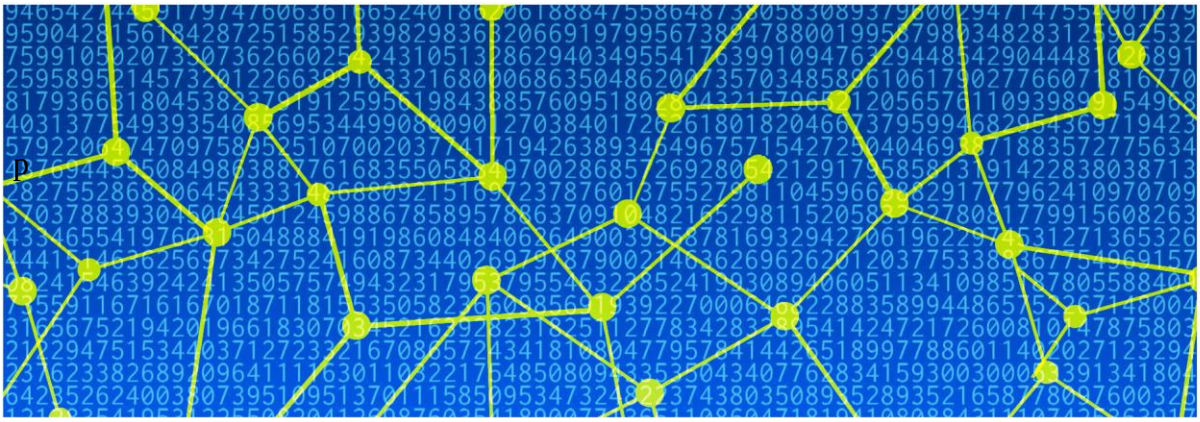

EUROPEAN DATA PROTECTION SUPERVISOR

Avis 6/2017

Avis du CEPD sur la proposition de règlement relatif à la vie privée et aux communications électroniques (le règlement «vie privée et communications électroniques»)

Le contrôleur européen de la protection des données (CEPD) est une institution indépendante de l'UE chargée, en vertu de l'article 41, paragraphe 2, du règlement nº 45/2001, «[e]n ce qui concerne le traitement de données à caractère personnel, [...] de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment leur vie privée, soient respectés par les institutions et organes communautaires», et «[...] de conseiller les institutions et organes communautaires et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel». Conformément à l'article 28, paragraphe 2, du règlement nº 45/2001, la Commission a l'obligation, lorsqu'elle adopte une proposition de législation relative à la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel, de consulter le CEPD.

Le CEPD et le contrôleur adjoint ont été nommés en décembre 2014 avec comme mission spécifique d'adopter une approche constructive et proactive. Le CEPD a publié en mars 2015 une stratégie quinquennale exposant la manière dont il entend mettre en œuvre ce mandat et en rendre compte.

Le présent avis fournit des observations et des recommandations sur la façon de mieux assurer la sauvegarde du droit au respect de la vie privée, de la confidentialité des communications ainsi que de la protection des données à caractère personnel dans la proposition de règlement relatif à la vie privée et aux communications électroniques, qui vise à abroger et à remplacer la directive «vie privée et communications électroniques» (2002/58/CE).

Synthèse

Le présent avis expose la position du CEPD sur la proposition de règlement relatif à la vie privée et aux communications électroniques, qui doit abroger et remplacer la directive «vie privée et communications électroniques».

Sans le règlement «vie privée et communications électroniques», le cadre réglementaire de l'UE en matière de respect de la vie privée et de protection des données serait incomplet. Le règlement général sur la protection des données (ci-après le «RGPD») constitue certes une avancée importante, mais il est nécessaire de disposer d'un outil juridique spécifique pour protéger le droit au respect de la vie privée garanti par l'article 7 de la Charte des droits fondamentaux, dont la confidentialité des communications constitue une composante essentielle. Dès lors, le CEPD approuve et se réjouit de la proposition, qui vise précisément à fournir un tel outil. Le CEPD soutient également le choix de l'instrument juridique, à savoir un règlement qui sera directement applicable et qui contribuera à garantir un niveau d'harmonisation et de cohérence accru. Il se félicite de l'ambition d'assurer un niveau élevé de protection tant en ce qui concerne le contenu que les métadonnées, et il soutient l'objectif consistant à étendre les obligations de confidentialité à un plus grand nombre de services, et notamment aux services de communication dits «par contournement» («OTT»), ce qui reflète l'évolution des technologies. Il considère également que la décision de n'accorder des pouvoirs de contrôle qu'aux seules autorités compétentes en matière de protection des données, conjuguée à la mise en place de mécanismes de coopération et de cohérence au sein du futur comité européen de la protection des données (le «comité»), contribuera à une application plus cohérente et plus effective des règles de l'Union.

En même temps, le CEPD doute qu'en l'état actuel, la proposition puisse effectivement tenir sa promesse de garantir un niveau élevé de protection de la vie privée dans les communications électroniques. En effet, nous avons besoin d'un nouveau cadre juridique pour la vie privée et les communications électroniques, mais ce cadre doit être plus intelligent, plus clair et plus solide. Il reste encore beaucoup à faire car, comme le rappelle la proposition, les règles sont d'une complexité redoutable. Les communications sont divisées en plusieurs catégories de données: métadonnées, données relatives au contenu et données émises par des équipements terminaux. Chacune de ces catégories bénéficie d'un niveau de confidentialité différent et est soumise à des exceptions différentes. Cette complexité pourrait entraîner un risque d'écarts, peut-être involontaires, en matière de protection.

La plupart des définitions sur lesquelles repose la proposition seront négociées et arrêtées dans le cadre d'un instrument juridique distinct: le code des communications électroniques européen. Aujourd'hui, il n'y a pas de justification juridique pour que ces deux instruments soient liés aussi étroitement et les définitions du code, qui sont centrées sur la concurrence et le marché, ne sont tout simplement pas adaptées au contexte des droits fondamentaux. Le CEPD préconise, dès lors, d'inclure un ensemble de définitions nécessaires dans le règlement «vie privée et communications électroniques», qui tiennent compte à la fois de la portée et des objectifs visés par le règlement.

Il convient également d'accorder une attention particulière à la question du traitement des données de communications électroniques par des responsables du traitement autres que les fournisseurs de services de communications électroniques. Les protections supplémentaires assurées aux données de communications seraient inutiles s'il était possible de les contourner facilement, par exemple en transférant les données à des tiers. Il convient, en outre, de s'assurer

que les règles en matière de vie privée et de communications électroniques n'aboutissent pas à un niveau de protection plus faible que celui consacré par le RGPD. Ainsi, par exemple, le consentement devrait être véritable: les utilisateurs doivent disposer d'une liberté de choix, comme l'exige le RGPD. Il ne devrait plus y avoir d'accès subordonné à l'acceptation du traçage («*tracking walls*»). En outre, les nouvelles règles devraient fixer des exigences strictes en ce qui concerne la vie privée dès la conception et par défaut. Enfin, le CEPD aborde également d'autres enjeux urgents dans le présent avis, notamment les limitations de la portée des droits.

TABLE DES MATIÈRES

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16,

vu la Charte des droits fondamentaux de l'Union européenne, et notamment ses articles 7 et 8,

vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et vu le 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 (le règlement général sur la protection des données),

vu le règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, et notamment son article 28, paragraphe 2, son article 41, paragraphe 2, et son article 46, point d),

A ADOPTÉ L'AVIS SUIVANT:

1. INTRODUCTION ET CONTEXTE

Le présent avis (ci-après l'«avis») fait suite à la demande adressée par la Commission européenne (ci-après la «Commission») au Contrôleur européen de la protection des données (ci-après le «CEPD»), en tant qu'autorité de contrôle indépendante et organe consultatif, afin d'obtenir son avis sur la proposition de règlement relatif à la vie privée et aux communications électroniques[1] (ci-après la «proposition»). La proposition vise à abroger et à remplacer la directive 2002/58/CE sur la vie privée et les communications électroniques (ci-après la directive «vie privée et communications électroniques»)[2]. La Commission a également sollicité l'avis du groupe de travail «Article 29» sur la protection des données (ci-après le «G29»), auquel le CEPD a contribué en tant que membre à part entière[3].

Le présent avis fait suite à l'avis préliminaire 5/2016 du CEPD sur le réexamen de la directive «vie privée et communications électroniques» (2002/58/CE)[4], rendu le 22 juillet 2016. Le CEPD est également susceptible de donner son avis aux stades ultérieurs de la procédure législative.

La proposition est l'une des initiatives clés de la stratégie pour un marché unique numérique[5], qui vise à renforcer la confiance dans les services numériques et leur sécurité dans l'Union européenne, en veillant tout particulièrement à garantir un niveau élevé de protection aux citoyens et des conditions de concurrence équitables pour l'ensemble des opérateurs du marché dans toute l'Union.

La proposition a pour but de moderniser et d'actualiser la directive «vie privée et communications électroniques» dans le cadre d'une stratégie plus large visant à établir un cadre juridique cohérent et harmonisé pour la protection des données en Europe. La directive «vie privée et communications électroniques» précise et complète la directive 95/46/CE[6], qui sera remplacée par le règlement général sur la protection des données (RGPD)[7], récemment adopté.

Dans un premier temps, le CEPD résume au chapitre 2 ses principales observations sur la proposition en se concentrant sur ses aspects positifs. Dans un second temps, au chapitre 3, il expose ses principales inquiétudes et formule des recommandations quant aux réponses à y apporter. D'autres inquiétudes et des recommandations en vue d'améliorations supplémentaires sont décrites dans l'annexe du présent avis, qui examine la proposition de façon plus détaillée. Le fait de répondre aux inquiétudes soulevées dans cet avis et son annexe et d'améliorer encore le texte du règlement «vie privée et communications électroniques» permettrait non seulement de mieux protéger les utilisateurs finaux et autres personnes concernées, mais aussi de procurer une plus grande sécurité juridique à l'ensemble des parties intéressées.

2. LA NÉCESSITÉ D'UN INSTRUMENT JURIDIQUE DÉDIÉ EN MATIÈRE DE VIE PRIVÉE ET DE COMMUNICATIONS ÉLECTRONIQUES

2.1 Les principaux aspects positifs de la proposition

Le CEPD se réjouit de la proposition de la Commission, qui vise à moderniser, à mettre à jour et à renforcer le règlement «vie privée et communications électroniques». Il partage le point de vue, exprimé à plusieurs reprises également par le G29 dans son avis préliminaire et dans des avis plus récents[8], ainsi que par certains groupes de la société civile dans leur analyse préliminaire et dans une analyse commune plus récente[9], selon lequel il existe un besoin constant de règles spécifiques pour protéger la confidentialité et la sécurité des communications électroniques dans l'Union européenne et pour compléter et préciser les exigences du RGPD. Il considère également qu'il est impératif de mettre en place des dispositions juridiques simples, ciblées et neutres du point de vue technologique, qui soient garantes, dans un avenir proche, d'une protection forte, intelligente et effective.

Le CEPD se réjouit également du fait que nombre des remarques qu'il a formulées dans son avis préliminaire et dans ses observations informelles aient été prises en compte, ce qui a contribué de façon notable à la qualité de la proposition. Il se félicite de l'ambition affichée par la proposition de garantir un niveau élevé de protection à l'égard du contenu et des métadonnées, et en particulier:

- du choix d'un règlement plutôt que d'une directive comme forme d'instrument juridique, ce qui pourrait contribuer à assurer un niveau de protection plus cohérent dans toute l'Union européenne;
- de l'extension du champ d'application aux fournisseurs de services OTT;
- de l'approche consistant à n'autoriser le traitement que dans des conditions clairement définies;
- de la modernisation des exigences de consentement actuelles en vertu des nouveaux articles 9 et 10;
- du recentrage des dispositions de sécurité sur les questions spécifiques aux services de communication et de l'alignement complet de la proposition sur le RGPD concernant les violations de données;
- du choix consistant à confier le contrôle de l'application des règles du RGPD et du règlement «vie privée et communications électroniques» aux mêmes autorités de contrôle;
- et de la règle du consentement préalable pour toutes les communications commerciales non sollicitées.

2.2 La confidentialité des communications électroniques doit rester protégée

Le droit à la confidentialité des communications est un droit fondamental protégé par l'article 7 de la charte des droits fondamentaux de l'Union européenne (ci-après la «charte»), l'équivalent moderne des lois (postales) classiques garantissant le secret de la correspondance[10].

La confidentialité des communications est essentielle au fonctionnement des sociétés et des économies modernes: sans messagers dignes de confiance qui transmettent des informations aux destinataires sans les utiliser à leurs propres fins, les divulguer à des tiers, en modifier le contenu ou supprimer ou retarder leur transmission, de nombreuses activités privées et publiques pourraient uniquement être effectuées de personne à personne.

Si l'importance économique et sociale de la fiabilité des communications ne saurait être surestimée, la protection du droit fondamental à la vie privée contre toute interférence, en particulier des autorités publiques, constitue sa fonction juridique centrale.

Pour garantir la sécurité juridique, il est fondamental de se doter de règles claires et spécifiques en droit dérivé afin de mettre en pratique le principe de confidentialité des communications électroniques. Il ne suffit pas de s'en remettre, au niveau de l'Union européenne, à un seul article de la charte. Dans le cadre juridique actuel, la directive «vie privée et communications électroniques» est l'instrument de la législation secondaire de l'UE qui énonce les obligations légales nécessaires et spécifiques.

La reconnaissance, dans la charte, de la confidentialité des communications en tant que droit fondamental est conforme aux traditions constitutionnelles européennes: la majorité des États membres de l'Union européenne reconnaissent également la confidentialité des communications comme un droit constitutionnel distinct[11]. De nouvelles dispositions, davantage harmonisées au niveau de l'Union européenne, contribuent à renforcer la sécurité juridique. Elles profitent en tant que telles aux personnes physiques, qui se voient offrir la même protection partout en Europe, ainsi qu'aux entreprises, en particulier celles qui exercent leurs activités dans plusieurs pays.

2.3 Le niveau actuel de protection ne doit pas être réduit

Outre la mise en œuvre du droit fondamental au respect de la vie privée concernant les communications électroniques, le règlement «vie privée et communications électroniques» doit également servir à garantir le droit fondamental à la protection des données à caractère personnel conformément à l'article 8 de la charte. Ce point est particulièrement important pour les situations dans lesquelles la directive «vie privée et communications électroniques» prévoit des garanties plus concrètes que celles prévues par le RGPD, afin d'assurer un niveau de protection plus élevé pour les données à caractère personnel et de contrer les risques spécifiques liés aux données de communications.

Ainsi, par exemple, alors que le RGPD ne définit pas spécifiquement quels fondements juridiques peuvent être permis pour le traitement et dans quelles situations, la directive «vie privée et communications électroniques» et la proposition de règlement «vie privée et communications électroniques» sont plus précises puisqu'elles imposent, dans certains contextes spécifiques, le consentement comme base juridique[12].

De même, il est essentiel que les nouvelles règles n'abaissent pas le niveau de protection en-deçà des protections instaurées par le RGPD, en créant des dérogations aux règles du RGPD.

De plus, outre les droits fondamentaux des personnes physiques, la proposition garantit la protection de certains des droits des personnes morales. Cela concerne les communications non sollicitées ainsi que d'autres aspects liés à leur rôle d'abonné ou d'utilisateur de services de communications électroniques. Si le RGPD ne couvre pas ces besoins[13], cette protection est essentielle au vu de l'importance cruciale de la mise en place de communications électroniques fiables et sécurisées pour assurer le bon fonctionnement de la société et de l'économie[14].

2.4 Des règles simples et claires sont nécessaires pour garantir la cohérence et la sécurité juridique

Le règlement «vie privée et communications électroniques» doit également veiller à ce que la nouvelle réglementation prévoie des règles simples et claires, qui soient appliquées de manière effective et uniforme partout en Europe. De ce point de vue, le CEPD se réjouit tout particulièrement des aspects suivants de la proposition.

Le choix d'un règlement plutôt que d'une directive

Le CEPD se félicite du fait que, comme il l'avait recommandé dans son avis préliminaire, les législateurs aient choisi un règlement plutôt qu'une directive comme support du nouvel instrument juridique. Ce choix est conforme à l'approche adoptée dans le RGPD. En effet, il garantit un niveau de protection plus cohérent et plus uniforme pour les personnes physiques et morales protégées par ses dispositions. En outre, il permet de fournir des conditions de concurrence équitables pour les organisations qui doivent respecter ses dispositions et contribue à réduire les coûts de mise en conformité des organisations.

Contrôle et mise en application

Le CEPD se réjouit du fait que, comme il l'avait recommandé dans son avis préliminaire, l'article 18 de la proposition confère aux autorités compétentes en matière de protection le pouvoir de contrôler l'application du règlement «vie privée et communications électroniques»; il se félicite également de l'application du mécanisme de coopération et de cohérence prévu par le RGPD aux questions relevant du champ d'application du règlement «vie privée et communications électroniques». De même, il accueille favorablement l'harmonisation accrue des pouvoirs de contrôle, et notamment du niveau des amendes[15].

La nécessité de règles simples et claires

La directive «vie privée et communications électroniques» et la nouvelle proposition prévoient des règles pour plusieurs situations dans lesquelles il pourrait être extrêmement compliqué de déterminer s'il y a traitement de données à caractère personnel et qui est le responsable du contrôle ou du traitement, et qui pourraient être les personnes concernées. Cela concerne, entre autres, les circonstances techniques liées à certaines opérations de réseau (par exemple, l'identification de l'appelant), l'intégrité des points terminaux des utilisateurs (informations sur les terminaux des utilisateurs) et l'utilisation de services de communications à des fins de prospection directe.

Dès lors, le CEPD se félicite de ce que la proposition, comme précédemment la directive «vie privée et communications électroniques», apporte une solution à ces situations en définissant les rôles et les actions liés à l'utilisation des services de communications sans qu'aucune analyse ne soit nécessaire en vertu du RGPD. Comme les dispositions de la directive «vie privée et

communications électroniques» ont fait l'objet d'interprétations très diverses, le règlement «vie privée et communications électroniques» permet de clarifier certains termes ou concepts.

2.5 Il est essentiel d'étendre le champ d'application du règlement «vie privée et communications électroniques»

Nous nous réjouissons de l'ambition affichée par la Commission d'étendre le champ d'application de la protection et de mettre à jour les règles de façon à couvrir de nouvelles façons de fournir les services de communications. Le maintien pur et simple de la protection actuellement disponible viderait ces droits de leur substance pour une partie sans cesse croissante de nos communications quotidiennes.

Messagerie instantanée et voix sur IP

Comme cela a déjà été mentionné dans notre avis préliminaire, les personnes physiques doivent se voir accorder le même niveau de protection pour l'ensemble des services fonctionnellement équivalents, qu'ils soient fournis par des fournisseurs de téléphonie fixe traditionnelle, de téléphonie mobile ou de messagerie (SMS, MMS) d'un côté, ou par des fournisseurs de services de communications OTT tels que la voix sur IP (VoIP)[16] et les applications de messagerie instantanée, de l'autre.

Les utilisateurs ont souvent des attentes similaires en ce qui concerne le respect de la vie privée et la confidentialité de ces messages, et une violation de la confidentialité peut être tout aussi attentatoire à la vie privée. Ainsi, par exemple, les utilisateurs ont la possibilité de commencer une conversation en utilisant la fonction de messagerie d'un jeu vidéo, pour passer ensuite à un service de messagerie instantanée par contournement et s'échanger des SMS et des MMS sur leurs téléphones mobiles avant de finalement s'appeler d'un téléphone à l'autre. Tous ces différents types de communications peuvent passer par les mêmes appareils, à savoir les téléphones intelligents, et l'existence de cadres juridiques différents pour les services utilisés n'est en rien évidente ni même compréhensible pour l'utilisateur.

À la lumière de ce qui précède, le CEPD se réjouit du fait que le considérant 11 de la proposition reconnaisse la nécessité d'étendre le champ d'application aux services fonctionnellement équivalents et qu'il cite également quelques exemples de ces services, en particulier la «*voix sur IP, les services de messagerie et de courrier électronique web*».

Comme nous l'avions également recommandé dans notre avis préliminaire, il est nécessaire d'aller encore plus loin et de protéger non seulement les communications «*fonctionnellement équivalentes*» aux services fournis par les fournisseurs de services de télécommunications traditionnels, mais aussi les services qui offrent de nouvelles possibilités de communication, éventuellement de Façon complémentaire à d'autres services. Dans cette optique, il convient de s'assurer que les fonctionnalités de communications intégrées dans d'autres services (par exemple les fonctionnalités de messagerie dans les applications de jeux ou de rencontres) bénéficient également de la même protection.

De ce fait, le CEPD se réjouit tout particulièrement du fait que les services dits «*accessoires*» soient explicitement mentionnés et couverts par l'article 4, paragraphe 2, de la proposition.

L'internet des objets

En réalité, ce que nous appelons couramment l'«internet des objets» est essentiellement un «*internet des objets connectés aux personnes*». En effet, l'internet des objets comprend notamment les traceurs sportifs, les capteurs de santé, les dispositifs de communications personnelles, les téléviseurs intelligents, les voitures intelligentes et de nombreux autres dispositifs. Ils sont équipés de capteurs détectant le son, l'image, le mouvement et les paramètres physiques de leur propriétaire. Le fait qu'ils déclenchent parfois leurs transferts de données et leurs communications sans que leur propriétaire n'intervienne (ou sans même qu'il en soit conscient) ne saurait être un motif pour accorder une protection moindre à ces communications, souvent sensibles.

La protection de la confidentialité des communications ne devrait pas dépendre du fait que les personnes parlent ou écoutent, qu'elles écrivent ou lisent le contenu d'une communication, ou qu'elles se fient simplement aux caractéristiques de plus en plus intelligentes de leurs terminaux pour communiquer du contenu en leur nom. Normalement, le fournisseur de communications ne devrait pas se soucier de la finalité ou du contenu des communications, ni même être conscient de telles caractéristiques des messages et des autres communications transmises à travers ses services.

Le CEPD se réjouit du fait que l'article 2, paragraphe 1, de la proposition[17] précise que l'objet et le contenu d'une communication ne doivent pas affecter la protection de celle-ci en vertu du droit au respect de la vie privée. Le CEPD se félicite également de ce que le considérant 12 mentionne spécifiquement l'internet des objets et les communications de machine à machine, et vise à faire en sorte que la proposition couvre sans ambiguïté les communications de machine à machine dans le cadre de l'internet des objets, quel que soit le type de réseau ou le service de communications utilisé, sur tous les réseaux et dans tous les services qui relèvent de quelque autre manière du champ d'application du règlement.

Couverture de différents types de réseaux

Le CEPD se réjouit également de l'ambition de la Commission de faire entrer tous les réseaux et services accessibles au public dans le champ d'application des exigences de confidentialité. Celles-ci devraient couvrir, par exemple, les services de Wifi dans les hôtels, les restaurants, les cafés, les magasins, les trains, les aéroports et les réseaux offerts par les hôpitaux ou les universités aux utilisateurs de leurs principaux services (les patients ou les étudiants, respectivement), ainsi que l'accès Wifi offert par les entreprises à leurs visiteurs et hôtes et les bornes Wifi créées par les administrations publiques[18].

3. PRINCIPALES INQUIÉTUDES ET RECOMMANDATIONS

S'il se félicite de la proposition, le CEPD demeure préoccupé par un certain nombre de dispositions qui risquent de nuire à l'intention de la Commission d'assurer un niveau élevé de protection de la vie privée dans les communications électroniques. En particulier, le CEPD tient à exprimer les inquiétudes suivantes:

- les définitions contenues dans la proposition ne doivent pas dépendre de la procédure législative distincte relative à la directive établissant le code des communications électroniques européen[19] (ci-après la «proposition de CCEE»);

- les dispositions relatives au consentement de l'utilisateur final doivent être renforcées. Le consentement doit être demandé aux personnes physiques qui utilisent les services, qu'elles soient abonnées ou non à ces services, ainsi qu'à toutes les parties intervenant dans une communication. En outre, les autres personnes concernées qui n'interviennent pas dans les communications doivent également être protégées;
- il convient de s'assurer que la relation entre le RGPD et le règlement «vie privée et communications électroniques» ne crée pas de vide juridique en ce qui concerne la protection des données à caractère personnel. Les données à caractère personnel recueillies sur la base du consentement de l'utilisateur final ou d'un autre fondement juridique en vertu du règlement «vie privée et communications électroniques» ne doivent pas faire l'objet d'un traitement ultérieur en dehors du cadre d'un tel consentement ou d'une telle exception, sur le fondement d'un autre motif juridique qui serait prévu par le RGPD mais pas par le règlement «vie privée et communications électroniques»;
- la proposition n'affiche aucune ambition en ce qui concerne l'accès subordonné à l'acceptation du traçage («*tracking* walls») (également appelé «accès subordonné à l'acceptation de cookies» ou «*cookie walls*»). L'accès aux sites web ne doit pas être subordonné à l'obligation pour la personne concernée de «*consentir*» à être suivie sur les sites qu'elle visite. En d'autres termes, le CEPD appelle les législateurs à veiller à ce que le consentement soit vraiment donné librement;
- la proposition ne garantit pas que les navigateurs (et les autres logiciels mis sur le marché qui permettent d'effectuer des communications électroniques) seront configurés par défaut de manière à empêcher le suivi de l'empreinte numérique des personnes;
- les exceptions relatives au suivi de la localisation des équipements terminaux sont trop larges et ne sont pas assorties de garanties adéquates;
- la proposition prévoit la possibilité pour les États membres de mettre en place des restrictions. Ces restrictions exigent des garanties précises.

Ces principales inquiétudes, et les recommandations quant aux réponses à y apporter, sont exposées au chapitre 3.

3.1 Champ d'application et définitions

Le CEPD se réjouit de l'intention de définir le champ d'application matériel du règlement «vie privée et communications électroniques» en fonction de son objectif consistant à garantir une protection cohérente et complète des droits fondamentaux au respect de la vie privée, à la confidentialité des communications et à la protection des données. En créant un instrument autonome qui ne s'inscrit plus dans le cadre de règles relatives à la concurrence et au marché, il devient possible de définir le champ d'application du nouveau règlement «vie privée et communications électroniques» de telle manière que le champ d'application et les définitions s'articulent non pas autour de facteurs et d'enjeux économiques liés à la concurrence loyale et à l'utilisation efficace des ressources, mais autour de la protection des droits fondamentaux.

Les principaux concepts utilisés dans le règlement «vie privée et communications électroniques» doivent être soigneusement définis pour garantir la pleine efficacité du règlement. Le CEPD craint que cette efficacité ne soit affaiblie ou entravée par le manque de précision et de clarté de certaines des définitions, ainsi que par une dépendance inutile à la proposition de CCEE. En effet, cela risque de retirer des droits aux personnes concernées ou de limiter le champ d'application du règlement d'une manière injustifiée.

Éviter la dépendance aux définitions du CCEE

Lorsque le cadre juridique global des communications électroniques a été adopté en 2002, la directive «vie privée et communications électroniques» en faisait alors partie intégrante. Cependant, les législateurs se sont aperçus qu'un ensemble de définitions nécessaire à la création d'un marché concurrentiel et équitable pour les services de communications électroniques, et à la réalisation des finalités qui s'y rattachent, n'était pas entièrement adapté pour la protection des droits fondamentaux. En conséquence, les termes centraux du cadre réglementaire – tels que «*utilisateur*» et «*communication*» – ont été spécifiquement définis dans la directive «vie privée et communications électroniques» pour les besoins de cet instrument, s'écartant ainsi des définitions générales de la directive-cadre[20]. Si la réforme du cadre de 2009 a conservé intact le lien entre ces instruments, elle a également maintenu les définitions distinctes de la directive «vie privée et communications électroniques».

Avec l'actuel processus législatif, les législateurs sont confrontés à des propositions d'instruments qui sont beaucoup plus indépendantes les unes des autres:

- la proposition de CCEE comprend, en effet, des règles pour le marché des communications électroniques visant à garantir un véritable marché unique des communications, une utilisation efficace du spectre, des incitations à l'investissement dans le haut débit, des conditions de concurrence équitables pour les acteurs du marché, ainsi qu'une réglementation efficace;
- la proposition «vie privée et communications électroniques» vise, quant à elle, à procurer un niveau élevé de protection de la vie privée aux utilisateurs des services de communications électroniques, et à faire en sorte que les services numériques soient plus sûrs et suscitent davantage la confiance[21].

Contrairement aux exercices de 2002 à 2009, le réexamen de 2017 n'est pas destiné à préserver le caractère synchrone du processus législatif dans les différents domaines, mais distingue clairement les règles liées aux marchés de celles liées à la protection des droits fondamentaux. En conséquence, les cadres dans lesquels les organes législatifs travaillent sur ces propositions ne sont pas toujours identiques, ce qui rend encore plus difficile la coordination des deux procédures.

Le CEPD se félicite de la distinction établie entre la dimension des droits fondamentaux et la dimension économique, et il se réjouit de la création d'un instrument spécifique et indépendant visant à protéger les droits fondamentaux au respect de la vie privée et à la protection des données des personnes physiques utilisant des services de communications électroniques. Le CEPD appelle toutefois les législateurs à appliquer pleinement la logique d'une telle approche. À cet égard, le CEPD ne juge pas nécessaire que les définitions de la proposition de CCEE soient automatiquement applicables dans ce contexte. En effet, le critère déterminant pour définir le champ d'application du règlement «vie privée et communications électroniques» devrait être la protection des droits fondamentaux, et pas uniquement les facteurs économiques liés à la concurrence loyale et à l'utilisation efficace des ressources. En outre, même si certaines définitions peuvent être identiques dans le texte des deux propositions, il serait préférable, en raison du contexte spécifique à la protection des droits fondamentaux, d'inclure dans le règlement «vie privée et communications électroniques» des définitions entièrement autonomes et, au besoin, de les préciser. Cela permettra également d'éviter que la signification des dispositions du règlement soit modifiée par les changements apportés au processus législatif sur le CCEE, sans préjudice de la cohérence nécessaire entre ces deux domaines législatifs.

La dépendance des définitions clés de la proposition à la procédure législative parallèle et distincte de la proposition de CCEE entraîne des risques inutiles et évitables pour la clarté et l'efficacité du règlement «vie privée et communications électroniques». En effet, tant que la proposition de CCEE ne sera pas adoptée, ses définitions peuvent toujours être modifiées. Or, si ces définitions sont utilisées dans la proposition «vie privée et communications électroniques», elles pourraient affecter la signification et l'incidence de ses dispositions. Comme cela a été observé par le passé, les définitions créées à des fins de réglementation économique ne sont, en général, pas censées être adaptées pour la protection des droits fondamentaux. **Pour ces raisons, le CEPD recommande, d'une part, de supprimer la dépendance inutile à la proposition de CCEE et, d'autre part, de définir des termes centraux, dans le règlement «vie privée et communications électroniques» lui-même, qui concordent avec la proposition de CCEE, sans pour autant être forcément identiques. Cela permettrait également de faciliter la compréhension du règlement «vie privée et communications électroniques» par un utilisateur moyen.**

Identifier clairement les personnes concernées

Par exemple, la définition d'*«utilisateur final»* remplit une fonction centrale dans la proposition «vie privée et communications électroniques», dans la mesure où elle est censée désigner l'entité dont les droits fondamentaux doivent être protégés. Cependant, dans la proposition de CCEE, la définition d'*«utilisateur final»* renvoie aux personnes physiques *ou morales* qui ont conclu un contrat avec un fournisseur de services de communications électroniques et ne fournissent pas de services de communications électroniques[22]. L'usage du terme *«utilisateur final»* dans ce sens ne garantit pas que les droits fondamentaux de toutes les personnes physiques utilisant des services de communications électroniques seront protégés de manière adéquate. En ce qui concerne les droits fondamentaux des individus, la proposition devrait utiliser un terme défini précisément dans ce but, en faisant référence à *toute personne physique utilisant des services de communications électroniques sans être nécessairement abonnée à ces services*. Cette définition serait appropriée pour de nombreuses dispositions, y compris aux articles 6 et 8. Dans d'autres dispositions, la référence à une entité ayant une relation contractuelle avec un fournisseur de services est utile (par exemple, à l'article 15 sur les annuaires accessibles au public). Le chapitre 3.2 analyse plus en détail les risques liés au fait de confier les décisions sur les droits fondamentaux à des entités autres que les personnes concernées.

Apporter de la clarté sur les services couverts

Comme souligné au chapitre 2.5, le CEPD insiste sur le fait que l'extension du champ d'application *matériel* constitue une adaptation de la législation aux évolutions technologiques et économiques qui s'imposait depuis longtemps. Les personnes physiques devraient être en mesure de compter sur la confidentialité de leurs communications, qu'elles utilisent des SMS ou un service de messagerie web. Les définitions se rapportant aux différents sous-ensembles de services sont essentielles pour déterminer le champ d'application de l'instrument. L'adaptation de la définition de *«service de communications interpersonnelles»*, à l'article 4, paragraphe 2, pour y inclure également les services accessoires, est également accueillie avec une très grande satisfaction. Cette adaptation illustre très clairement le fait que le champ d'application du règlement «vie privée et communications électroniques» n'est pas destiné à être identique à celui de la proposition de CCEE et qu'il peut nécessiter des définitions spécifiques ou différentes de celles du CCEE. La question de savoir si le service utilisé pour

communiquer est central ou accessoire, du point de vue du fournisseur, n'est pas pertinente pour la protection de la confidentialité des communications.

S'assurer que toutes les données de communications sont couvertes

En ce qui concerne la définition des métadonnées de communications, la proposition mentionne uniquement, à l'article 4, paragraphe 3, point c), les «*données traitées dans un réseau de communications électroniques*». Cela pourrait entraîner un manque de protection lorsque certaines des données déterminant le traitement de contenus de communications sont traitées par des équipements qui font partie des infrastructures du service mais qui ne sont pas considérés comme faisant partie du réseau. Cela pourrait être le cas lorsque ces données sont traitées par des équipements considérés comme des *«ressources associées»* au sens du CCEE.

Afin d'éviter de tels écarts en matière de protection, la définition des métadonnées à l'article 4, paragraphe 3, point c), devrait englober non seulement les données traitées *«dans un réseau de communications électroniques»*, mais aussi celles traitées par d'autres équipements en vue de la fourniture du service et qui ne sont pas considérées comme du contenu.

En outre, du point de vue d'un fournisseur de communications soumis au règlement «vie privée et communications électroniques», le contenu ou la finalité d'une communication ne peut jouer un rôle dans le traitement de sa confidentialité et de sa sécurité. Le fournisseur ne devrait pas chercher à savoir si le message transmis consiste en la lecture d'un moniteur de fréquence cardiaque, un ordre de transaction boursière émis par une application intelligente d'opérations de marché ou une photo d'un bouquet de fleurs accompagnant une invitation à un mariage. L'efficacité et l'efficience des services, le respect de la vie privée et la sécurité doivent par conséquent être assurés pour l'ensemble des communications. Lorsque certains types de communications exigent des mesures spécifiques de la part du réseau, de nombreux protocoles de communications existants permettent de spécifier ces exigences dans le cadre des métadonnées de communications. Afin de garantir la fiabilité des services, il serait préférable d'appliquer cette méthode plutôt que de violer la confidentialité dans ce but.

Protéger les données de communications dans le «nuage»

Une autre préoccupation du CEPD est que le règlement «vie privée et communications électroniques» doit non seulement définir clairement la confidentialité et la sécurité des communications en transit, mais il doit également protéger la confidentialité et la sécurité des équipements des utilisateurs finaux et des données de communications stockées dans le *«nuage»*. **Le CEPD recommande de revoir l'article 5 et le considérant 15 de la proposition de manière à couvrir clairement ces deux situations.**

Dans sa rédaction actuelle, le considérant 15 de la proposition semble ne couvrir que les données en transit. En effet, il dispose que «*l'interdiction de l'interception des données de communication devrait s'appliquer durant leur acheminement, c'est-à-dire jusqu'à la réception du contenu de la communication électronique par le destinataire*».

Si l'article 8, paragraphes 1 et 2, protège également les communications stockées dans des équipements terminaux, le règlement devrait prévoir clairement le même niveau de protection pour les communications stockées dans d'autres équipements que les terminaux des utilisateurs, par exemple dans des boîtes de messagerie gérées par un fournisseur de services ou tout

stockage en nuage utilisé dans le cadre du service de communication[23]. En effet, le CEPD tient à souligner que les nouveaux paradigmes techniques (par exemple, l'informatique en nuage) renforcent encore plus l'importance de la confidentialité[24].

Comme expliqué par le G29 dans son avis 1/2017[25], le champ d'application de la protection défini dans le texte cité du considérant 15 est basé sur un cadre conceptuel de communications qui est dépassé. Aujourd'hui, la plupart des données de communications sont stockées par les fournisseurs de services, y compris après leur réception. Il conviendrait de faire en sorte que la confidentialité de ces données demeure protégée. En outre, la communication entre des abonnés aux mêmes services d'informatique en nuage (par exemple, les fournisseurs de messagerie web) ne nécessitera souvent que très peu de transmission: la plupart du temps, l'envoi d'un courrier électronique consisterait principalement en l'enregistrement du message dans la base de données du fournisseur, plutôt qu'en une transmission des communications entre deux parties.

Le CEPD recommande, plus généralement, de soumettre le corpus complet des définitions utilisées dans la proposition de règlement à un examen approfondi, afin d'éviter une dépendance inutile à la proposition de CCEE et de faire en sorte que le niveau de protection ne soit pas abaissé par rapport à celui prévu par l'actuelle directive «vie privée et communications électroniques».

3.2 Le consentement devrait être demandé aux personnes physiques dont les droits sont affectés

Le CEPD se réjouit de l'ambition affichée par la Commission d'assurer un niveau élevé de protection tant au contenu qu'aux métadonnées, en donnant au consentement, tel que défini dans le RGPD, un rôle central dans le traitement des données de communications électroniques au titre des articles 6 et 8 de la proposition.

Toutefois, dans certaines situations, ces dispositions permettraient à des tiers de donner leur consentement et donc de prendre des décisions concernant les droits fondamentaux d'autres personnes, ce qui irait à l'encontre de l'auto-détermination des personnes physiques et de l'essence même de la notion de «*consentement*» telle qu'elle est définie dans le RGPD.

Ainsi, si l'on s'en tient aux définitions de la proposition, le consentement de l'utilisateur final pourrait signifier, par exemple, qu'en tant qu'abonné, un employeur pourrait donner son consentement à la place des salariés qui utilisent les services. Cela concernerait aussi, de façon générale, d'autres situations dans lesquelles une organisation s'abonne à des services qui sont alors utilisés par des personnes physiques dans le cadre de cet abonnement, ou dans lesquelles un propriétaire fournit certains services de communications à ses locataires.

Pour ajouter à la complexité, la proposition n'exige pas simplement le consentement de l'«*utilisateur final*» pour le traitement des données. Au lieu de cela, elle utilise divers termes pour déterminer qui devrait donner son consentement:

- à l'article 6, paragraphe 2, point c), relatif aux métadonnées, il s'agit de l'«*utilisateur final concerné*»;
- à l'article 6, paragraphe 3, points a) et b), relatif au contenu, il s'agit soit de l'«*utilisateur ou [des] utilisateurs finaux concernés*» (en cas de fourniture d'un service spécifique à un utilisateur final), soit de
- «*tous les utilisateurs finaux concernés*» (dans tous les autres cas);

- à l'article 8, paragraphe 1, point b), relatif à la protection des équipements terminaux, il s'agit de l'«*utilisateur final»;*
- en revanche, aux articles 15 et 16 (annuaires accessibles au public et communications non sollicitées), il s'agit des «*utilisateurs finaux qui sont des personnes physiques*».

À la lumière de ce qui précède, et compte tenu du manque de clarté de la définition d'*«utilisateur final»* et des formulations peu cohérentes utilisées dans les différentes dispositions de la proposition relatives au consentement, il est difficile de savoir qui doit donner son consentement et dans quelle situation. Dans les trois sous-chapitres suivants, le CEPD explique ses trois principales inquiétudes en ce qui concerne la notion de consentement de l'utilisateur final, et il formule des recommandations pour répondre à chacune de ces inquiétudes.

Le consentement doit être donné par les personnes physiques qui utilisent le service

Premièrement, la proposition doit s'assurer que ce sont les personnes physiques qui utilisent effectivement le service de communications qui ont le droit de décider d'autoriser ou non le traitement de leurs données de communications.

Comme indiqué ci-dessus, les personnes qui s'abonnent à un service ne sont pas toujours celles (ou les seules personnes) qui utilisent le service. Ainsi, par exemple, un employeur pourrait s'abonner à des services qui seront ensuite utilisés par ses salariés ou par des visiteurs, ou une chaîne d'hôtels pourrait s'abonner à des services de communications en vue de leur utilisation par ses hôtes. De même, un propriétaire ou un chef de famille pourrait s'abonner à des services qui seront ensuite utilisés par plusieurs personnes physiques (par exemple, des membres de la famille ou des locataires) vivant dans les mêmes locaux (ainsi que par des visiteurs).

Nous supposons que la Commission avait l'intention de veiller à ce que ce soient les personnes physiques utilisant effectivement le service, et non celles qui y sont abonnées, qui donnent leur consentement. Néanmoins, ce point devrait être précisé dans la proposition.

À cet effet, le CEPD recommande d'inclure une définition autonome du terme *«utilisateur final»* dans le règlement «vie privée et communications électroniques» en vue du consentement au traitement des données de communications. Cette définition devrait s'articuler autour des quatre éléments suivants: i) *toute personne physique ii) utilisant un service de communications électroniques accessible au public iii) à des fins privées ou professionnelles, iv) sans être nécessairement abonnée à ce service»*[26].

En outre, nous recommandons d'inclure dans la proposition un considérant qui précise, à l'aide d'exemples spécifiques, que les utilisateurs finaux comprennent notamment les salariés, locataires, clients d'hôtels, membres de la famille, visiteurs, ainsi que toute autre personne physique utilisant effectivement les services, à des fins privées ou professionnelles, sans y être nécessairement abonnée.

Le consentement doit être demandé à toutes les parties intervenant dans une communication

Les règles proposées doivent également préciser qu'en règle générale, toutes les parties intervenant dans une communication, comme, par exemple, l'expéditeur et le destinataire d'un courrier électronique, ou toutes les personnes physiques participant à une vidéoconférence, doivent avoir la possibilité de décider d'autoriser ou non le traitement de leurs données de communications.

Le CEPD suppose que la Commission avait l'intention d'exiger, dans la plupart des cas typiques, comme pour la numérisation du contenu des courriers électroniques à des fins d'étude de marché ou de publicité ciblée, le consentement de toutes les parties intervenant dans une

communication. En même temps, le CEPD reconnaît qu'il pourrait y avoir des circonstances précises dans lesquelles le consentement d'une seule partie pourrait être suffisant (par exemple, lorsque les données de localisation d'une personne sont tracées sans avoir recours aux données à caractère personnel d'une autre personne, ou lorsqu'une personne demande des services limités spécifiques, comme la capacité d'effectuer des recherches et d'organiser ses courriels entrants selon des mots clés ou par expéditeur). Dans ces cas, il est possible de prévoir spécifiquement les exceptions éventuellement nécessaires[27].

À la lumière des considérations précédentes, et afin de simplifier la complexité de la proposition, le CEPD recommande d'utiliser systématiquement la même expression dans la proposition (*«tous les utilisateurs finaux»*) chaque fois que le consentement de l'utilisateur final est requis[28]. Cette approche systématique est particulièrement importante au regard des métadonnées et du contenu visés à l'article 6, ainsi que de tout traitement au titre de l'article 8[29].

Les droits de personnes physiques autres que les parties communicantes doivent également être protégés

Enfin, le CEPD s'inquiète également de la protection des personnes physiques qui n'interviennent pas dans une communication, mais dont les données à caractère personnel sont incluses dans ces communications[30]. Conformément au RGPD, tout traitement de données personnelles (en dehors des activités domestiques et autres exceptions) est subordonné à l'obligation de disposer d'un fondement juridique pour le traitement au titre de l'article 6[31].

Afin de dissiper toute ambiguïté quant à la mesure dans laquelle les dispositions du RGPD s'appliquent également à ces situations, **le CEPD recommande d'ajouter une disposition matérielle pour confirmer que *«le traitement basé sur le consentement de l'utilisateur final ne doit pas porter atteinte aux droits et libertés des personnes physiques dont les données à caractère personnel sont liées à la communication, et en particulier leurs droits au respect de la vie privée et à la protection des données à caractère personnel les concernant»*.**

3.3 La relation entre le RGPD et le règlement «vie privée et communications électroniques»

Le CEPD se réjouit du fait que, comme il l'avait recommandé précédemment, la relation entre le RGPD et le règlement «vie privée et communications électroniques» demeure complémentaire, comme c'est le cas actuellement. Les termes actuels: «*complètent et précisent*», qui ont désormais été ajoutés à l'article 1, paragraphe 3, de la proposition, sont satisfaisants pour définir cette relation[32].

Le CEPD se félicite également de ce que le considérant 5 précise désormais clairement que la proposition *«n'abaisse pas le niveau de protection dont bénéficient les personnes physiques en vertu [du RGPD]»*. Le CEPD recommande de renforcer encore cette phrase en ajoutant la formulation suivante pour exprimer le message d'une manière plus positive: *«au contraire, le cas échéant, il vise à fournir des garanties supplémentaires et complémentaires compte tenu de la nécessité de renforcer la protection de la confidentialité des communications»*.

Le CEPD constate toutefois que cette relation soulève la question suivante: dans le cas où l'utilisateur final a consenti à ce qu'un fournisseur de services transfère des métadonnées et/ou des données de contenu à un tiers qui agira alors en tant que responsable du traitement, le traitement des données par le tiers en question sera-t-il régi par le RGPD ou par le règlement «vie privée et communications électroniques»?

Les conséquences de ce choix sont importantes. En effet, si le RGPD s'appliquait au traitement ultérieur, tous les fondements juridiques du traitement prévus à l'article 6 du RGPD pourraient être invoqués par le tiers. En revanche, si la proposition était également applicable, le traitement ne serait possible que sur la base du consentement (ou d'une autre exception spécifique prévue par la proposition).

Si la proposition était interprétée comme signifiant que les tiers peuvent se prévaloir de tout fondement juridique prévu par le RGPD pour effectuer le traitement, cela créerait un vide juridique qui pourrait considérablement abaisser le niveau de protection prévu dans le règlement «vie privée et communications électroniques». Par exemple, les fournisseurs de services de communications (qui seraient couverts par la proposition) pourraient être tentés d'établir des filiales pour contourner le régime plus strict du règlement «vie privée et communications électroniques».

Afin de garantir la sécurité juridique, le CEPD recommande que la proposition précise, dans une disposition matérielle, que «*ni les fournisseurs de services de communications électroniques, ni les tiers ne peuvent traiter des données à caractère personnel collectées sur la base du consentement ou de tout autre motif juridique au titre du règlement "vie privée et communications électroniques", sur le fondement d'une autre base juridique qui ne serait pas spécifiquement prévue dans le règlement "vie privée et communications électroniques"».

Le CEPD recommande en outre d'inclure un considérant expliquant que *«lorsque le traitement est autorisé en vertu d'une exception aux interdictions prévues par le règlement "vie privée et communications électroniques", tout autre traitement sur la base de l'article 6 du RGPD est réputé interdit, y compris le traitement à d'autres fins sur le fondement de l'article 6, paragraphe 4, du RGPD. Cela n'empêcherait pas les responsables du traitement de demander un consentement supplémentaire en vue de nouveaux traitements».*

Cela ne devrait pas empêcher les législateurs de prévoir des exceptions supplémentaires, limitées et spécifiques dans le règlement «vie privée et communications électroniques», par exemple pour protéger les «*intérêts vitaux*» des personnes concernées conformément à l'article 6, point d), du RGPD, ou pour autoriser le traitement à des fins de recherche scientifique ou à des fins statistiques (officielles) aux termes de l'article 89 du RGPD[33].

En outre, la dernière phrase proposée du considérant 5 dispose que *«le traitement des données de communications électroniques par les fournisseurs de services de communications électroniques ne devrait être permis que conformément au présent règlement»*. Cette phrase crée une certaine ambiguïté dans la mesure où elle pourrait laisser entendre que le traitement de données de communications électroniques par des tiers autres que les fournisseurs de services de communications électroniques ne relève pas du champ d'application du règlement «vie privée et communications électroniques». Cela serait contraire à la lettre de l'article 2, paragraphe 1, et abaisserait le niveau de protection prévu par le règlement «vie privée et communications électroniques». Ce qui compte, ce n'est pas *qui* traite les données, mais *quel type de données* est protégé. Le traitement des données de communications électroniques et des informations liées aux équipements terminaux des utilisateurs devrait relever, sans ambiguïté, du champ d'application du règlement «vie privée et communications électroniques», quelle que soit l'entité chargée de traiter ces mêmes données. **En conséquence, le CEPD recommande de remplacer la phrase citée au considérant 5 par le texte suivant: *«le traitement des***

données de communications électroniques ne devrait être permis que conformément au présent règlement et à un fondement juridique spécifiquement prévu dans celui-ci».

3.4 Le consentement doit être donné librement: il faut en finir avec les «*tracking walls*»

Les «tracking walls» et la notion du consentement librement donné

L'article 8, paragraphe 1, qui est rédigé sur le modèle de l'article 5, paragraphe 3, de l'actuelle directive «vie privée et communications électroniques», interdit *«l'utilisation des capacités de traitement et de stockage des équipements terminaux et la collecte d'informations provenant des équipements terminaux des utilisateurs finaux, y compris sur les logiciels et le matériel»*. Les exceptions comprennent le cas dans lequel «*l'utilisateur final a donné son consentement*» conformément à l'article 8, paragraphe 1, point b).

Si le CEPD se réjouit de ces nouvelles dispositions et recommande le maintien de l'exigence de consentement actuelle, il reconnaît aussi que l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques», tel qu'il est appliqué actuellement, n'a pas pleinement concrétisé son potentiel d'offrir une véritable possibilité de choix et de donner le pouvoir de contrôle aux personnes physiques. Au lieu de cela, des entreprises et d'autres organisations ont mis au point des mécanismes de consentement dans le but de satisfaire sans doute aux exigences juridiques brutes de conformité prévues par la directive «vie privée et communications électroniques», mais sans véritablement donner aux utilisateurs la possibilité de choisir et de contrôler ce qu'il advient de leurs données.

Ce phénomène est parfois désigné sous le terme d'«accès subordonné à l'acceptation du traçage» ou «*tracking walls*». Les *tracking walls* ont pour effet d'empêcher les utilisateurs qui n'acceptent pas le suivi sur d'autres sites d'accéder aux sites web qu'ils veulent consulter[34]. Les cookies et autres techniques, telles que la prise d'empreintes numériques, servent à suivre en permanence la trace numérique laissée par les utilisateurs sur l'internet. Les sociétés qui y ont accès utilisent ensuite les informations ainsi collectées à des fins de profilage et de publicité et à d'autres fins commerciales. Ce traçage généralisé, soi-disant basé sur le consentement, comporte de graves risques pour la vie privée et dépossède totalement les personnes physiques concernées du contrôle de leurs données à caractère personnel.

Les *tracking walls* mettent à mal l'idée du libre consentement, une exigence clé prévue à la fois par la directive 95/46/CE et par le RGPD. Le RGPD améliore la directive 95/46/CE non seulement en exigeant que le consentement soit donné librement, mais aussi en fournissant des orientations supplémentaires sur ce que cela signifie dans les faits. Il prévoit, en particulier, que le consentement n'est pas considéré comme ayant été donné librement dans des situations où la fourniture d'un service est subordonnée au consentement de la personne concernée au traitement de ses données à caractère personnel, en dépit du fait que ce traitement n'est pas nécessaire à la prestation du service en question[35]. Tel est précisément le cas des *tracking walls*, qui obligent souvent l'utilisateur à consentir à l'utilisation de cookies de traçage de tiers qui ne sont pas nécessaires à la prestation du service concerné. Il est essentiel que les utilisateurs soient en mesure d'utiliser un service sans être tracés, en particulier par des tiers et dans des situations où l'utilisateur dépend de l'utilisation du service et n'a pas d'alternative réelle à celui-ci. Il est possible d'affirmer, sur la base du RGPD, que ces *tracking walls* sont totalement interdits en raison de l'absence d'un consentement éclairé *«donné librement»*. Pour garantir la sécurité juridique, il est important que cela soit mentionné explicitement dans le règlement «vie privée et communications électroniques».

Compte tenu de l'importance d'un consentement donné librement et de l'application souvent insuffisante de l'article 5, paragraphe 3, par les exploitants de sites web, le CEPD recommande une interdiction totale et explicite desdits «*tracking walls*».

En conséquence, le CEPD recommande que le règlement «vie privée et communications électroniques» prévoie, dans une disposition matérielle, que *«nul ne peut se voir refuser l'accès à des services de la société de l'information (que ces services soient payants ou non) au motif qu'il ou elle n'a pas donné le consentement visé à l'article 8, paragraphe 1, point b), au traitement de données à caractère personnel qui ne sont pas nécessaires à la fourniture de ces services».*

Pour compléter cette disposition, le CEPD recommande, en outre, une interdiction supplémentaire et explicite de la pratique consistant à exclure les utilisateurs qui disposent d'applications permettant de bloquer les publicités ou autres et de modules d'extension installés pour protéger leurs informations et leurs équipements terminaux.

Pour éviter toute confusion, le CEPD recommande l'ajout d'un considérant confirmant explicitement que *«le traitement des données aux fins de la fourniture de publicités ciblées ne peut être considéré comme nécessaire à l'exécution d'un service».*

Un autre motif d'inquiétude est que les utilisateurs finaux pourraient également être confrontés à des mécanismes de consentement forcé avant qu'ils ne puissent commencer à utiliser des appareils intelligents (comme les téléviseurs intelligents). Dans le contexte de l'internet des objets, il convient de faire en sorte que la fonctionnalité des dispositifs intelligents ne soit pas subordonnée à un consentement qui n'est pas nécessaire à la fonctionnalité demandée. Le but est de préciser les conditions de l'article 7, paragraphe 4, du RGPD en les adaptant au contexte de l'internet des objets, où les utilisateurs finaux achètent et utilisent des produits physiques dont ils peuvent raisonnablement attendre certaines fonctionnalités.

Le CEPD recommande donc d'introduire également une interdiction similaire et spécifique dans la proposition, sous la forme d'une disposition matérielle précisant que *«nul ne peut se voir refuser une fonctionnalité d'un dispositif de l'internet des objets (que l'utilisation de ce dispositif soit payante ou non) au motif qu'il ou elle n'a pas donné le consentement visé à l'article 8, paragraphe 1, point b), au traitement de données qui ne sont pas nécessaires à la fonctionnalité demandée».*

Cette approche complète garantirait le niveau de protection le plus élevé pour les personnes physiques, ainsi que la sécurité juridique et des conditions de concurrence équitables à tous les acteurs économiques.

Autres modèles commerciaux fondés sur la transparence et la responsabilisation des utilisateurs

Cette approche n'est pas incompatible avec une utilisation et une réutilisation innovantes des données à caractère personnel dans le domaine des *«données massives»*. Elle vise plutôt à renforcer les droits fondamentaux, tout en envisageant des possibilités nouvelles qui permettront aux entreprises de développer des services innovants basés sur les données à caractère personnel et reposant sur une confiance mutuelle. La transparence du mode d'utilisation et de réutilisation des données à caractère personnel par les organisations doit être renforcée, et les personnes physiques doivent bénéficier d'un contrôle accru sur ce qu'il advient

de leurs données. Comme le CEPD l'a affirmé dans son avis intitulé «*Relever les défis des données massives*»[36], les entreprises et les autres organisations qui déploient d'importants efforts dans la recherche de solutions innovantes pour l'utilisation des données à caractère personnel devraient faire preuve du même esprit innovant dans la mise en œuvre des principes de protection des données.

Les compagnies téléphoniques, les fournisseurs de services web ainsi que les autres organisations qui fournissent des services de communications relevant du champ d'application du règlement «vie privée et communications électroniques» sont souvent les mieux à même de construire une relation mutuellement bénéfique, fondée sur la confiance, avec leurs clients. Dans le cadre de cette relation de confiance, les clients pourraient être prêts à collaborer et à partager leurs données à caractère personnel pour des usages nouveaux et innovants qui profitent à toutes les parties intéressées[37].

3.5 La vie privée doit être protégée par défaut

Le CEPD soutient fermement la précision apportée à l'article 9, selon laquelle le consentement peut être exprimé à l'aide des paramètres techniques si cela est techniquement possible et réalisable. Toutefois, pour assurer l'efficacité de cette disposition, les exigences relatives au respect de la vie privée par défaut sont également essentielles. De tels outils doivent être proposés à l'utilisateur lors de la configuration initiale, à l'aide de paramètres par défaut respectueux de la vie privée, et à chaque fois que les utilisateurs apportent des modifications importantes à leurs dispositifs ou logiciels. En outre, toutes les parties concernées, y compris les exploitants du site web, devraient être obligées d'adhérer aux normes techniques et aux normes sur le respect des politiques communément admises[38].

Comme l'a souligné le CEPD dans son avis préliminaire[39], les utilisateurs doivent disposer de mécanismes efficaces et faciles à utiliser pour donner et retirer leur consentement. Dès lors, le CEPD se félicite du fait que la proposition dispose que le consentement de l'utilisateur au traitement peut être exprimé à l'aide des paramètres appropriés d'un navigateur ou d'une autre application.

En principe, l'article 9, paragraphe 2, de la proposition prévoit une approche utile en ce qui concerne l'utilisation des paramètres de configuration technique du dispositif d'un utilisateur et des logiciels installés sur l'appareil pour exprimer le consentement. La formulation de l'article 9, paragraphe 2, de la proposition: «*sans préjudice du paragraphe 1*» vise à faire en sorte que tout mécanisme de consentement facile à utiliser respecte également les exigences du RGPD, et notamment un degré de spécificité suffisant et la possibilité pour la personne concernée de retirer son consentement

À l'inverse, l'article 10 de la proposition exige que les utilisateurs finaux aient la «*possibilité*» de déterminer, à l'aide des paramètres du logiciel, s'ils autorisent des tiers à accéder à des données ou à en stocker dans leurs dispositifs. Le CEPD considère que cette disposition est contraire à l'article 25 du RGPD sur la «*Protection des données dès la conception et protection des données par défaut*». **Au lieu de cela, le CEPD recommande que la proposition impose l'obligation, pour les fournisseurs de matériel et de logiciels, de mettre en œuvre des paramètres par défaut qui protègent les dispositifs des utilisateurs finaux contre tout accès non autorisé à des informations ou tout stockage d'informations dans leurs dispositifs.**

En outre, le CEPD recommande d'ajouter une disposition matérielle instaurant l'obligation, pour l'ensemble des parties concernées, y compris les exploitants de sites web,

d'adhérer aux normes techniques et aux normes sur le respect des politiques communément admises.

L'article 10, paragraphe 2, oblige les fournisseurs de logiciels à informer les utilisateurs des paramètres de confidentialité disponibles au moment de la première utilisation du logiciel. Il est essentiel que, durant ce processus, les utilisateurs aient la possibilité de faire un simple choix pour éviter d'être tracés. Toutefois, cette même approche du «*tout ou rien*» ne devrait pas s'appliquer à leur consentement au traçage. Comme souligné ci-dessus, les moyens techniques utilisés pour donner le consentement doivent respecter les exigences de consentement énoncées à l'article 4, paragraphe 12, du RGPD, et notamment la règle selon laquelle le consentement doit non seulement être *«donné librement»*, mais doit également être «*spécifique*» et *«éclairé»*. Fournir des informations générales sur les paramètres de confidentialité, lors de la première utilisation d'un logiciel, qui auront un impact de type *«tout ou rien»* sur toute utilisation ultérieure, ne répondra pas aux exigences de consentement prévues par le RGPD.

En outre, il est important que les utilisateurs soient informés des paramètres de confidentialité lors de l'installation ou de la première utilisation du logiciel, mais aussi à chaque fois qu'ils effectuent des modifications ultérieures importantes dans leurs dispositifs ou leurs logiciels. De tels avis devraient également être fournis, par exemple, lorsque les utilisateurs restaurent les réglages par défaut de leurs dispositifs. Dans ces cas-là, les paramètres devraient également rester réglés de façon à garantir le respect de la vie privée par défaut. Ils devraient aussi être aisément accessibles durant l'utilisation.

3.6 Les dispositifs ne doivent pas être tracés sans le consentement de leurs utilisateurs

Le CEPD s'inquiète également de l'exception proposée à l'article 8, paragraphe 2, point b), du règlement «vie privée et communications électroniques», visant à tracer les utilisateurs de dispositifs de communication dans des espaces publics du monde réel (parfois désigné par le terme «*traçage de dispositifs*»). Ce type de technologie est déjà utilisé, notamment, pour mesurer la fréquentation de centres commerciaux ou pour cartographier les flux du trafic routier. Si les données collectées sont souvent destinées à être utilisées à des fins statistiques, elles peuvent aussi révéler la localisation et les habitudes comportementales de personnes physiques. Dans certains contextes, par exemple à proximité d'un établissement religieux ou d'une clinique médicale, les données de localisation sont en elles-mêmes extrêmement sensibles, même sous leur forme brute, sans profilage ni analyse poussés.

Compte tenu des risques potentiels pour la vie privée, il est inquiétant que la proposition prévoie une autorisation quasi-totale de ce type de traçage, la seule condition étant qu'un message soit transmis à l'utilisateur l'informant des mesures qu'il peut prendre pour *«réduire au minimum la collecte ou la faire cesser»*.

On voit mal pourquoi cette forme d'utilisation des données de localisation devrait bénéficier d'une protection moindre que les autres. Ailleurs dans la proposition, les fournisseurs de services de communications ne sont autorisés à traiter les informations concernant la localisation des utilisateurs qu'à la condition que ceux-ci aient donné leur consentement. Les données traitées dans le contexte du traçage de dispositifs dans le monde réel ne devraient pas être considérées comme moins sensibles.

Par rapport à un traitement basé sur un consentement préalable («*opt-in*»), une solution fondée sur l'opposition au traitement («*opt-out*») offre une protection moindre en raison de la prégnance de l'option *«par défaut»:* la plupart des personnes n'auront tout simplement ni le temps ni l'envie de signifier leur opposition: elles accepteront l'option par défaut et ne s'opposeront pas au traitement. Au-delà de cette inquiétude plus générale, l'approche proposée,

à savoir la notification, alliée à une forme d'opposition faible et inefficace, est problématique, et ce, pour plusieurs raisons.

Premièrement, un utilisateur peu attentif pourrait ne même pas remarquer le message affiché dans un espace très fréquenté. Par ailleurs, si cette technologie fait l'objet d'une application à grande échelle, l'utilisateur pourrait ne recevoir la notification qu'aux abords d'un tel espace, ce qui rendrait l'existence de ladite technologie encore plus invisible.

Deuxièmement, compte tenu des formulations de la proposition, les utilisateurs pourraient n'avoir la possibilité de se soustraire à ce type de traçage qu'en désactivant les fonctionnalités de base de leurs propres dispositifs, comme l'accès internet sans fil de leurs téléphones mobiles. On ne saurait attendre de l'utilisateur qu'il signifie son opposition – peut-être même plusieurs fois – lorsqu'il entre dans un espace où sont utilisées des technologies de traçage de dispositifs. C'est d'autant plus vrai si l'opposition au traçage se fait au détriment des fonctionnalités des dispositifs de l'utilisateur. Dans ce contexte, il importe également de mettre l'accent sur le message énoncé au considérant 18, qui traite du contenu: « *L'accès Internet à haut débit de base [...] [doit] être considéré comme un service essentiel pour que les individus puissent communiquer et bénéficier des avantages de l'économie numérique. Le consentement relatif au traitement de données [...] ne sera pas valable si la personne concernée ne dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice»*.

En outre, s'il est techniquement possible de signifier son opposition a posteriori, par exemple, en enregistrant l'adresse MAC Wifi du dispositif dans une base de données vérifiée par le fournisseur du service de suivi de la localisation, ce même procédé peut être utilisé pour un régime de consentement préalable. Le consentement éclairé donné librement, comme l'exige le RGPD, est préférable dans tous les cas.

À la lumière de ce qui précède, le CEPD recommande de supprimer les paragraphes 2, point b), 3 et 4, de l'actuel article 8 et de les remplacer par une exigence de consentement simplifiée (de la part de tous les utilisateurs finaux[40] concernés). De plus, comme à l'article 6 régissant le traitement du contenu et des métadonnées, le règlement «vie privée et communications électroniques» devrait également préciser que le traitement fondé sur le consentement n'est possible que si les finalités *«ne peuvent être atteintes en traitant des informations rendues anonymes*[41]*»*.

Si nécessaire, des exceptions limitées et ciblées pourraient être prévues à des fins de recherche scientifique et de statistiques (officielles) en vertu de l'article 89 du RGPD, et aux fins de la sauvegarde des «intérêts vitaux» des personnes physiques conformément à l'article 6, point d), du RGPD[42].

Une exception supplémentaire, limitée et étroitement ciblée pourrait également être prévue à des fins de comptage de personnes (par exemple, pour mesurer la fréquentation des stades de football ou les flux de trafic), sous réserve de garanties appropriées, y compris des mesures techniques et organisationnelles pour veiller à ce que les données traitées dans ce but ne soient pas traitées à d'autres fins, et en particulier qu'elles ne soient pas traitées pour soutenir des mesures ou des décisions prises à l'égard de l'individu concerné («*séparation fonctionnelle*»)[43], d'une possibilité horizontale effective de s'opposer au traitement [similaire à une «liste rouge» («*do not call*») dans le contexte des communications non sollicitées ou à un registre

d'«opposition au traçage» («*do not track*») dans le contexte du traçage en ligne], ainsi que de limitations strictes quant à la durée de conservation des données.

Le CEPD recommande également que le règlement «vie privée et communications électroniques» mentionne spécifiquement la possibilité pour le comité de fournir des orientations supplémentaires concernant les garanties à mettre en œuvre. Ces orientations plus détaillées pourraient notamment recommander que, dans des cas typiques d'utilisation à des fins statistiques, les identifiants du dispositif final de l'utilisateur ne soient jamais stockés ni traités directement, mais qu'ils servent uniquement de base pour calculer de nouveaux identifiants pseudonymes, ou encore que ces identifiants ne puissent pas être croisés entre différents services de traçage et qu'ils aient une persistance très courte, limitée à ce qui est strictement nécessaire pour effectuer les calculs statistiques.

3.7. Les restrictions doivent être limitées et soumises à des garanties

L'article 11 de la proposition correspond pour l'essentiel à l'actuel article 15 de la directive «vie privée et communications électroniques». L'article 15, paragraphe 1, de la directive «vie privée et communications électroniques» autorise les États membres, entre autres, à mettre en œuvre un régime national de conservation des données prévoyant le stockage obligatoire des données de communications électroniques par les fournisseurs pour assurer la détection, la recherche et la poursuite d'infractions graves, y compris le terrorisme. Depuis l'annulation, dans l'arrêt *Digital Rights* de 2014[44], de la directive 2006 sur la conservation des données (2006/24/CE)[45], les États membres ne sont plus soumis à l'obligation, au titre d'un instrument législatif spécifique de l'Union, d'introduire ou de maintenir un régime de conservation des données.

Le CEPD tient à rappeler que tout régime national de conservation des données doit respecter les dispositions de la charte, et notamment des articles 7, 8, 11, 47 et 52, comme prévu dans la jurisprudence pertinente de la Cour de justice. En particulier, les États membres devraient se conformer à la jurisprudence de l'arrêt *Digital Rights Ireland*, y compris le dernier arrêt rendu dans *Tele 2 Sverige* et *Watson et autres*[46].

En outre, le CEPD partage l'approche adoptée dans la proposition, selon laquelle seuls certains des motifs énumérés à l'article 23, paragraphe 1, du RGPD peuvent être acceptés comme fondements juridiques pour limiter la portée de certains droits et obligations énoncés aux articles 5 à 8 de la proposition. En effet, intégrer *tous* les motifs d'exception visés à l'article 23 du RGPD ne serait pas approprié étant donné la spécificité de la proposition par rapport au RGPD[47].

En tout état de cause, le CEPD considère que le simple fait que la portée visée par la proposition soit étendue par rapport à celle de l'actuelle directive «vie privée et communications électroniques» ne devrait pas être interprété comme un mandat général autorisant les États membres à étendre systématiquement le champ d'application de tout régime de conservation des données (existant ou à venir) au-delà des services de communications électroniques traditionnels relevant actuellement du champ d'application de l'article 15, paragraphe 1, de la directive «vie privée et communications électroniques». Il conviendrait, tout au moins, de démontrer la nécessité et la proportionnalité de telles obligations en matière de conservation des données, en conformité avec la charte et la jurisprudence de la Cour mentionnée précédemment[48].

Garanties supplémentaires

L'article 23, paragraphe 2, du RGPD dispose que les mesures législatives imposant des limitations doivent contenir des dispositions spécifiques comme, par exemple, l'explication des finalités du traitement et les garanties destinées à prévenir les abus et l'accès ou le transfert illicites. Il devrait être indiqué très clairement que les spécifications et garanties supplémentaires prévues à l'article 23, paragraphe 2, doivent également s'appliquer aux cas où des limitations sont imposées en vertu du règlement «vie privée et communications électroniques». Ce point devrait être précisé dans une disposition matérielle de la proposition[49].

En outre, étant donné que les éventuelles limitations affecteront non seulement les droits des personnes physiques à la protection de leurs données à caractère personnel, mais aussi la confidentialité des communications, le CEPD **recommande aux législateurs de vérifier attentivement quelles garanties spécifiques sont requises en vertu de la proposition.**

En particulier, dans les cas où l'article 23, paragraphe 1, point e), du RGPD s'applique, le CEPD recommande que la proposition dispose que les mesures législatives imposant des limitations devraient être subordonnées à l'obtention d'une autorisation judiciaire préalable pour tout accès au contenu ou aux métadonnées[50].

Transparence concernant les demandes d'accès émanant de pouvoirs publics

Dans les réseaux mondiaux, les communications traversent les frontières sans que les utilisateurs en soient conscients. Les communications entre les États membres de l'Union européenne peuvent traverser des pays tiers, tandis que les communications entre pays tiers peuvent être transmises en passant par le territoire de l'Union. Les fournisseurs de services de communications établis ou exerçant leurs activités dans l'Union européenne peuvent être saisis de demandes d'informations ou d'accès concernant les données de leurs utilisateurs introduites par les services répressifs ou de sécurité d'autres États membres et de pays tiers, en vertu de leurs pratiques et de leurs législations nationales applicables, ce qui crée des exceptions au droit à la confidentialité des communications. Après l'entrée en vigueur du RGPD, ces demandes de transfert de données à caractère personnel vers un pays tiers pourront être fondées uniquement sur un accord international tel qu'un traité d'entraide judiciaire[51].

Le recours aux pouvoirs des services de sécurité et de répression pour violer la confidentialité des communications doit être conforme aux principes de nécessité et de proportionnalité. Si l'information des personnes physiques faisant l'objet de telles mesures peut être restreinte, par exemple pour protéger les objectifs d'une enquête en cours, une connaissance générale de la fréquence et de l'ampleur des demandes de divulgations adressées aux fournisseurs de services de communications donnerait aux citoyens en général, mais aussi aux organismes publics, la possibilité de comparer et d'évaluer la pratique générale liée à l'utilisation de ces instruments. La transparence autour des demandes d'accès émanant de pouvoirs publics peut donc jouer un rôle important pour contribuer à garantir le respect des droits fondamentaux.

En conséquence, le CEPD a déjà recommandé dans son avis préliminaire que le règlement «vie privée et communications électroniques» prévoie des règles spécifiques visant à renforcer la transparence[52]. Il a recommandé en particulier qu'une nouvelle disposition fasse obligation aux organisations de divulguer, au moins à intervalles réguliers et sous une forme agrégée, les demandes d'informations émanant de services répressifs et d'autres pouvoirs publics. Cette

obligation devrait s'appliquer aux demandes émanant aussi bien de l'intérieur que de l'extérieur de l'Union européenne. Nous avons également expliqué qu'en ce qui concerne les demandes émanant de pays tiers, les fournisseurs de services devraient respecter la condition de légalité prévue à l'article 48 du RGPD.

Si le CEPD se réjouit du fait que l'article 11, paragraphe 2, prend des mesures qui vont dans le sens d'une plus grande transparence en permettant à l'autorité de contrôle compétente d'accéder, sur demande, à certaines informations concernant ces procédures, il recommande aux législateurs d'aller encore plus loin en matière de transparence et d'exiger la publication de ces informations.

En outre, le CEPD recommande que les autorités de contrôle bénéficient non seulement d'un accès «*sur demande*» à ces informations, mais qu'elles se voient remettre d'office des rapports périodiques.

4. CONCLUSIONS

Le CEPD se réjouit de la proposition de la Commission tendant à moderniser, à mettre à jour et à renforcer le règlement «vie privée et communications électroniques». Il partage le point de vue selon lequel il existe un besoin constant de règles spécifiques pour protéger la confidentialité et la sécurité des communications électroniques dans l'Union européenne et pour compléter et préciser les exigences du RGPD. Il considère également qu'il est impératif de mettre en place des dispositions juridiques simples, ciblées et neutres du point de vue technologique, qui soient garantes, dans un avenir proche, d'une protection forte, intelligente et effective.

Le CEPD se félicite de l'ambition affichée de garantir un niveau élevé de protection à l'égard du contenu et des métadonnées, et il se réjouit en particulier des principaux éléments positifs exposés à la section 2.1.

S'il se félicite de la proposition, le CEPD demeure préoccupé par un certain nombre de dispositions qui risquent de nuire à l'intention de la Commission d'assurer un niveau élevé de protection de la vie privée dans les communications électroniques. En particulier, le CEPD tient à exprimer les inquiétudes suivantes:

- les définitions contenues dans la proposition ne doivent pas dépendre de la procédure législative distincte relative à la directive établissant le code des communications électroniques européen[53] (ci-après la «proposition de CCEE»);
- les dispositions relatives au consentement de l'utilisateur final doivent être renforcées. Le consentement doit être demandé aux personnes physiques qui utilisent les services, qu'elles soient abonnées ou non à ces services, ainsi qu'à toutes les parties intervenant dans une communication. En outre, les personnes concernées qui n'interviennent pas dans les communications doivent également être protégées;
- il convient de s'assurer que la relation entre le RGPD et le règlement «vie privée et communications électroniques» ne crée pas de vide juridique en ce qui concerne la protection des données à caractère personnel. Les données à caractère personnel recueillies sur la base du consentement de l'utilisateur final ou d'un autre fondement juridique en vertu du règlement «vie privée et communications électroniques» ne doivent pas faire l'objet d'un traitement ultérieur en dehors du cadre d'un tel consentement ou d'une telle exception, sur le fondement d'un autre motif juridique qui

serait prévu par le RGPD mais pas par le règlement «vie privée et communications électroniques»;

- la proposition n'affiche aucune ambition en ce qui concerne l'accès subordonné à l'acceptation du traçage («*tracking* walls») (également appelé «accès subordonné à l'acceptation de cookies» ou «*cookie walls*»). L'accès aux sites web ne doit pas être subordonné à l'obligation pour la personne concernée de «*consentir*» à être suivie sur les sites qu'elle visite. En d'autres termes, le CEPD appelle les législateurs à veiller à ce que le consentement soit vraiment donné librement;
- la proposition ne garantit pas que les navigateurs (et les autres logiciels mis sur le marché qui permettent d'effectuer des communications électroniques) seront configurés par défaut de manière à empêcher le suivi de l'empreinte numérique des personnes;
- les exceptions relatives au suivi de la localisation des équipements terminaux sont trop larges et ne sont pas assorties de garanties adéquates;
- la proposition inclut la possibilité pour les États membres d'instaurer des limitations; celles-ci exigent des garanties précises.

Ces principales inquiétudes, ainsi que les recommandations concernant les réponses à y apporter, sont exposées dans le présent avis. Au-delà des observations générales et des principales inquiétudes énoncées dans le corps de l'avis, le CEPD formule en annexe des commentaires et des recommandations supplémentaires, et parfois plus techniques, sur la proposition, dans le but notamment de faciliter le travail des législateurs et des autres parties intéressées qui souhaitent encore améliorer le texte durant le processus législatif. Enfin, nous tenons également à souligner l'importance d'un traitement rapide de ce dossier capital par les législateurs, de façon à ce que le règlement «vie privée et communications électroniques» puisse s'appliquer, comme prévu, à compter du 25 mai 2018, date à laquelle le RGPD entrera lui aussi en vigueur.

L'importance de la confidentialité des communications consacrée à l'article 7 de la charte ne cesse d'augmenter compte tenu du rôle accru que les communications électroniques jouent dans notre société et notre économie. Les garanties exposées dans le présent avis joueront un rôle déterminant dans la réalisation des objectifs stratégiques à long terme que la Commission a décrits dans les grandes lignes dans sa stratégie pour un marché unique numérique.

Fait à Bruxelles, le 24 avril 2017

(**signature**)

Giovanni BUTTARELLI

Contrôleur européen de la protection des données

ANNEXE: ANALYSE APPROFONDIE ET RECOMMANDATIONS

Au-delà des observations générales et des principales inquiétudes exposées dans le corps de l'avis, le CEPD tient également à formuler des commentaires et des recommandations supplémentaires, et parfois plus techniques, sur la proposition, dans le but notamment de fournir un outil de travail qui facilitera le travail des législateurs et des autres parties intéressées qui souhaitent encore améliorer le texte durant le processus législatif.

Pour faciliter leur consultation, l'ordre de ces observations et de la discussion suit la structure de la proposition, en commençant par les considérants avant de passer aux différents articles.

1. La couverture des différents types de réseaux (considérant 13)

Comme souligné ci-dessus à la section 2.5, le CEPD se réjouit également de l'ambition de la Commission de faire entrer tous les réseaux et services accessibles au public dans le champ d'application des exigences de confidentialité. Le considérant 13 comprend ainsi plusieurs exemples, comme *«… les bornes Wi-Fi situées à différents endroits des villes, grands magasins, centres commerciaux et hôpitaux»*.

Pour éviter toute ambiguïté, le CEPD encourage le législateur à ajouter des précisions et des exemples supplémentaires. Ces exemples devraient comprendre, par exemple, les services de Wifi fournis dans les hôtels, restaurants, cafés, magasins, trains, aéroports et les réseaux offerts par les universités à leurs étudiants, ainsi que l'accès Wifi offert par les entreprises à leurs visiteurs et hôtes et les bornes Wifi créées par les administrations publiques.

En outre, le CEPD recommande également que le considérant 13 précise ce qui devrait être considéré comme *«accessible au public»*. Par exemple, il conviendrait de clarifier qu'un service est considéré comme accessible au public même si le fournisseur restreint le service aux utilisateurs enregistrés, comme dans le cas d'une organisation offrant l'accès au Wifi à ses clients et visiteurs[54].

2. Les données à caractère personnel ne peuvent pas être considérées comme une contrepartie (considérant 18)

Le considérant 18 de la proposition «vie privée et communications électroniques» dispose que *«dans l'économie numérique, les services sont souvent fournis moyennant une contrepartie non pécuniaire, par exemple l'exposition de l'utilisateur final aux publicités».* Cela peut impliquer que les données des utilisateurs finaux soient utilisées comme une contrepartie, notamment si ce considérant est lu en combinaison avec le considérant 16 de la proposition de CCEE, qui suggère de façon plus directe que les *«services de communications électroniques sont souvent fournis en échange d'une contrepartie non pécuniaire, par exemple l'octroi de l'accès aux données à caractère personnel ou à d'autres données»*.

Le CEPD souligne que les données à caractère personnel ne peuvent être considérées comme une *«contrepartie»* pour une demande de service, comme l'accès à un site web ou à une application. La raison en est que le consentement n'est valable que s'il est donné librement et retiré sans porter préjudice à la personne concernée. Comme le CEPD l'a récemment expliqué dans son avis 4/2017 sur la proposition relative au contenu numérique[55], la notion de «*contrepartie*» instaure des obligations supplémentaires pour la personne et n'est ni cohérente, ni compatible avec la notion de consentement au titre du RGPD. En effet, les notions de

«paiement en données à caractère personnel» et de données à caractère personnel proposées comme *«contrepartie»* porteraient atteinte aux fondements juridiques actuels du traitement licite, tels qu'ils sont exposés à l'article 6 du RGPD.

Le CEPD recommande donc de supprimer la formulation citée du considérant 18 et de la modifier comme suit: «*Dans l'économie numérique, les services sont souvent fournis contre une rémunération payée par un tiers plutôt que par le destinataire du service*».

3. Toutes les personnes physiques ont besoin de protection, pas seulement les citoyens (considérant 33)

Le CEPD recommande de remplacer le terme «*citoyen*» par le terme «*personne physique*» au considérant 33. Le concept de citoyenneté n'est pas approprié pour ce qui est de protéger les droits fondamentaux, car toutes les personnes physiques de l'UE ont le droit de bénéficier d'une protection aux termes de la charte, pas seulement les citoyens.

4. La protection des personnes morales (article 1)

S'il est clairement justifié que les personnes morales jouissent également de droits concernant leurs communications électroniques et que la protection de ces droits devrait être intégrée dans la proposition, il convient néanmoins d'apporter des modifications au texte de la proposition. La référence aux droits et libertés fondamentaux des *«personnes morales»* à l'article 1, paragraphe 1, devrait être supprimée. Au lieu de cela, en ce qui concerne les personnes morales, le CEPD recommande d'utiliser des formulations similaires à celles utilisées à l'article 1, paragraphe 2, de l'actuelle directive «vie privée et communications électroniques».

5. Le champ d'application territorial devrait correspondre à celui du RGPD (article 3)

Le CEPD recommande que le règlement «vie privée et communications électroniques» dispose, sans ambiguïté, du même champ d'application *territorial* que le RGPD (y compris le champ d'application extraterritorial visé à l'article 3, paragraphe 2[56]) et qu'il suive la même approche en ce qui concerne le droit applicable au traitement des données à caractère personnel. Si le libellé actuel de l'article 3 ne s'oppose pas à une telle interprétation, il ne permet pas de savoir clairement si le champ d'application territorial prévu est identique, et, par conséquent, la disposition devrait être modifiée de façon à couvrir le même domaine. Un considérant permettrait de préciser davantage les intentions du législateur.

La reproduction mot pour mot des dispositions du RGPD ne permettrait pas d'atteindre le but recherché, dans la mesure où l'application du règlement «vie privée et communications électroniques» ne devrait pas être subordonnée au fait que les parties concernées soient qualifiées de *«responsable du traitement»* ou de *«sous-traitant»* au sens du RGPD.

6. «Messages échangés via une plateforme» (article 4, paragraphe 1, point b), et considérant 1)

Le CEPD se réjouit du fait que le considérant 1 confirme que le principe de confidentialité s'applique aux «*moyens de communication actuels et futurs*» et donne des exemples comme les *«appels téléphoniques, l'accès à Internet, les applications de messagerie instantanée, le courrier électronique, les appels téléphoniques par Internet et la messagerie personnelle fournie par les réseaux sociaux»*.

Le CEPD partage la demande de clarification formulée par le G29 dans son avis 1/2017[57]. En effet, la proposition devrait inclure spécifiquement, et sans ambiguïté, tous les messages échangés via une plateforme entre les utilisateurs d'un même réseau social (comme Facebook ou Twitter).

Le CEPD recommande également que ce considérant précise de manière plus claire que la notion de communication n'inclut pas seulement les communications électroniques entre deux personnes physiques (ou machines), mais aussi toute communication au sein d'un groupe défini (par exemple, une audioconférence ou des messages envoyés à un groupe défini de destinataires).

En outre, comme il l'a souligné à la section 3.1 ci-dessus à propos du champ d'application et des définitions, le CEPD recommande d'introduire des définitions distinctes, indépendantes et mieux adaptées à la protection de la vie privée et de la confidentialité des communications, afin que les messages échangés via une plateforme soient inclus, sans ambiguïté, dans la notion de «*service de communications interpersonnelles*», et, partant, dans la définition de «*service de communications électroniques*[58].

7. Définition de «*courrier électronique*» (article 4, paragraphe 3, point e)

Le CEPD recommande de remplacer le terme défini «*courrier électronique*» par un terme plus général, comme, par exemple, «*message électronique*», à l'article 4, paragraphe 3, point e), afin qu'il n'y ait pas de confusion avec les mots «*courrier électronique ou courriel*», qui sont couramment utilisés. La clarté de la définition est essentielle pour garantir la sécurité juridique en ce qui concerne la portée de la protection contre les communications non sollicitées prévue à l'article 16[59].

Le considérant 33 proposé souligne avec raison la nécessité que les dispositions sur les communications non sollicitées soient neutres sur le plan technologique. Le CEPD se félicite de la mention spécifique dans ce considérant, à titre d'exemple, des «*applications de messagerie instantanée, courriels, SMS, MMS, [et] Bluetooth*». Nous encourageons également le législateur à fournir d'autres exemples dans ce considérant. Ainsi, dans le cadre de la protection contre les communications non sollicitées, il conviendrait notamment de veiller à ce que les personnes physiques soient protégées contre tous les messages non sollicités, qu'ils soient livrés à l'aide de la fonction «*chronologique*» ou de la fonction de messagerie d'un réseau social ou d'une application de jeux.

Pour garantir la sécurité juridique, la définition elle-même doit être suffisamment claire et large pour que le terme défini englobe tous les canaux de communication pertinents, en plus des communications de courrier électronique traditionnelles[60].

8. Le traitement au titre des exceptions doit être «*strictement*» nécessaire (articles 6 et 8, paragraphe 1)

Le CEPD approuve les recommandations du G29 selon lesquelles, en ce qui concerne les exceptions visées aux articles 6 et 8, paragraphe 1, de la proposition de règlement, le mot «*strictement*» devrait être ajouté avant «*nécessaire*»[61].

9. Exception à des fins de sécurité (article 6, paragraphe 1, point b))

L'article 6, paragraphe 1, point b), autorise le traitement du contenu et des métadonnées à des fins de sécurité. Le CEPD rappelle, comme indiqué dans la présente annexe, à la section 8 ci-dessus, que cette exception doit être interprétée de manière étroite et limitée à ce qui est strictement nécessaire. Suivant ces principes, le contenu ne peut être traité qu'aux fins de reconnaître et de supprimer les éléments susceptibles d'être dangereux pour le réseau ou le terminal de l'utilisateur lui-même, par exemple des virus ou autres éléments malveillants, mais pas à d'autres fins. Cela n'exclut pas qu'un traitement supplémentaire à ces fins puisse être autorisé sur la base du consentement des personnes physiques concernées et sous réserve d'autres garanties comme celles mentionnées à l'article 6, paragraphe 3, point b). Le CEPD tient également à rappeler l'avis 2/2006 du G29 sur les problèmes de protection de la vie privée liés à la fourniture de services de filtrage du courrier électronique[62].

10. La protection des métadonnées de communications doit être renforcée (article 6, paragraphe 2)

Le CEPD attire l'attention du législateur sur le fait qu'il n'existe pas de distinction claire entre le contenu et les «*métadonnées*» dans un environnement multiservices tel que l'internet, dans lequel le service fourni à l'utilisateur combine souvent divers composants technologiques d'une manière telle que ce qui est considéré comme du contenu pour un composant constitue des métadonnées pour un autre[63].

Le traitement de données concernant la communication (comme les adresses URL des sites web consultés, l'intitulé du courriel, les numéros de téléphone appelés, la localisation des équipements terminaux) est souvent tout aussi révélateur que le contenu même de la communication. Les métadonnées concernant les communications peuvent fournir un profil très détaillé d'une personne physique et leur traitement peut être tout aussi attentatoire à la vie privée que le traitement du contenu des communications.

Par exemple, les métadonnées permettent l'identification de cibles lors d'opérations militaires à l'aide de drones[64]. Les métadonnées peuvent également servir à identifier des structures dans le cadre d'attentats politiques et d'enquêtes pénales[65]. Des recherches ont, en outre, établi que des personnes physiques peuvent être identifiées à partir d'une suite très limitée de données de localisation tirées d'un téléphone mobile[66]. Il a également été prouvé que des informations intimes au sujet du mode de vie et des convictions d'une personne, tels que ses tendances et fréquentations politiques, ses problèmes médicaux, son orientation sexuelle et ses pratiques religieuses peuvent être découverts à partir des données relatives au trafic tirées de son téléphone mobile[67].

En outre, pour certains types de données, la question de savoir si elles peuvent être considérées comme du contenu ou des métadonnées a été discutée au titre de la directive «vie privée et communications électroniques». Le considérant 2 de la proposition précise désormais qu'une URL complète (indiquant la page web visitée) est considérée comme des métadonnées. Toutefois, compte tenu de la nature sensible de ces données, ce type de données devrait bénéficier du même niveau élevé de protection que les données de contenus.

Comme cela a été expliqué également par le G29 dans son avis 1/2017[68], le règlement «vie privée et communications électroniques» doit donc clairement prévoir un niveau élevé de protection de la confidentialité des communications tant pour le «*contenu*» que pour les

«*métadonnées*». La proposition reconnaît cette nécessité au considérant 2, ce dont le CEPD se réjouit.

Malgré son ambition d'assurer un niveau élevé de protection des métadonnées, la proposition permet le traitement de ces données sous réserve de garanties moins strictes. Pour garantir un niveau élevé de protection, le CEPD recommande que les mêmes règles de consentement soient applicables tant au contenu qu'aux métadonnées au titre de l'article 6.

11. La protection des équipements terminaux: la nécessité de formulations neutres et inclusives du point de vue technologique (article 8)

Le CEPD se félicite du fait que la formulation retenue pour l'article 8, paragraphe 1, peut être considérée comme neutre et inclusive du point de vue technologique, comme cela a été recommandé dans l'avis préliminaire[69].

Le CEPD rappelle la nécessité de veiller à ce que toutes les techniques de traçage, actuelles et futures, utilisées par l'intermédiaire de téléphones intelligents et d'applications de l'IdO soient pleinement couvertes. Les règles devraient, en particulier, couvrir la prise d'empreintes numériques, ainsi que toutes les formes de «traçage passif», c'est-à-dire l'utilisation d'identifiants et d'autres données diffusées par les appareils. Avec le développement de l'internet des objets, de plus en plus de données seront susceptibles d'être diffusées «par défaut». Plutôt que de prévoir, comme condition, que les informations soient «déjà stockées, dans l'équipement terminal», il serait envisageable de couvrir l'ensemble des informations susceptibles d'être obtenues à partir de l'appareil. Les opérations concernées nécessiteraient un consentement, sauf dans le cas de la transmission et de la fourniture d'un service, comme cela est prévu actuellement, ainsi qu'une éventuelle extension dans le cas, très rare, d'un traitement directement lié à un service demandé par l'utilisateur et exécuté exclusivement par le fournisseur de services.

12. Exception pour «*mesurer des résultats d'audience sur le web*» (article 8, paragraphe 1, point d))

Dans l'avis préliminaire, le CEPD a recommandé que le règlement «vie privée et communications électroniques» devrait également prévoir une exception supplémentaire pour les témoins analytiques d'origine, sous réserve de garanties adéquates[70]. Cette exception devrait permettre de garantir que les données peuvent être traitées lorsque le traitement n'affecte pas, ou peu, le droit de l'utilisateur à la confidentialité de ses communications et à la vie privée. Le CEPD recommandait de limiter de telles exceptions aux cas où l'utilisation de ce genre de témoins analytiques d'origine sert strictement à des fins de statistiques agrégées. En outre, des garanties adéquates doivent être appliquées, notamment la communication d'informations claires aux personnes physiques concernées, un mécanisme facile à utiliser permettant de ne pas participer à tout traitement de données et des techniques d'anonymisation appropriées appliquées aux informations collectées telles que les adresses IP. Dans son avis 04/2012 sur l'exemption de l'obligation de consentement pour certains cookies[71], le G29 a déjà appelé les législateurs à établir une telle exception.

Le CEPD a également recommandé que, pour de plus amples orientations sur les garanties devant être appliquées et les conditions auxquelles un témoin analytique d'origine peut être exempté de l'exigence de consentement, le règlement «vie privée et communications électroniques» pourrait faire référence aux orientations futures qui seront fournies par le comité européen de la protection des données.

Le CEPD se réjouit de l'instauration d'une nouvelle exception. Toutefois, afin que l'exception demeure limitée, le CEPD recommande d'ajouter la formulation *«et pour autant qu'aucune donnée à caractère personnel ne soit rendue accessible à des tiers»* à la fin du paragraphe. Cette formulation vise à ce que l'exception fasse l'objet d'une interprétation restreinte et exclue spécifiquement l'utilisation des services de tiers, comme prévu et recommandé par le G29.

Le CEPD relève également que l'exception ne doit pas créer de vide juridique pour le stockage à long terme ou le traitement ultérieur des données à caractère personnel à des fins supplémentaires. Autoriser le stockage d'informations dans les équipements de l'utilisateur ou la lecture d'informations depuis les équipements de l'utilisateur à des fins statistiques n'est acceptable que si un certain nombre de conditions sont remplies. Les informations qui en résultent pourraient, par exemple, ne pas donner une image détaillée des différents utilisateurs, et les informations obtenues ne doivent pas être utilisées dans un but autre que celui de mieux comprendre le fonctionnement et l'utilisation, d'une manière agrégée et générale, d'un service. De même, les informations ne doivent pas être fusionnées avec d'autres informations pour développer un profil d'utilisateur, ni être utilisées pour cibler l'utilisateur.

La proposition devrait être mise à jour de façon à inclure des garanties essentielles et devrait mentionner la possibilité pour le comité d'élaborer des orientations supplémentaires[72]. Ainsi, par exemple, dans le cas du traçage de dispositifs (comme évoqué à la section 3.6 du corps du présent avis), le CEPD recommande que cette exception soit soumise à des garanties supplémentaires, y compris des mesures techniques et organisationnelles pour veiller à ce que les données traitées à ces fins ne soient pas traitées à d'autres fins, et en particulier qu'elles ne soient pas traitées pour soutenir des mesures ou des décisions prises à l'égard de l'individu concerné, ainsi qu'à une possibilité horizontale effective de s'opposer au traitement et à des limitations strictes quant à la durée de conservation des données.

13. Recommandations supplémentaires concernant le traçage de dispositifs (article 8, paragraphe 2)

Premièrement, le CEPD recommande de supprimer la formulation *«pour permettre sa connexion à un autre dispositif ou à un équipement de réseau»* de la première phrase de l'article 8, paragraphe 2, afin de garantir une couverture neutre du point de vue technologique et une protection complète de toutes les données émises par des équipements terminaux, indépendamment de la finalité.

Deuxièmement, le CEPD recommande d'ajouter la formulation *«autorisée par les utilisateurs finaux concernés»* (ou similaire) après *«dans le but d'établir une connexion».* L'objectif est de s'assurer que la connexion établie est bien celle dont l'utilisateur a connaissance et à laquelle il a donné son consentement préalable. Par exemple, certaines personnes pourraient avoir accepté, via les paramètres appropriés de leur dispositif, que chaque fois qu'elles sont près d'une borne Wifi, leur dispositif recherche automatiquement les réseaux disponibles (préalablement spécifiés), voire qu'il s'y connecte automatiquement. En même temps, elles pourraient ne pas autoriser leur traceur médical ou de fitness à communiquer leurs informations médicales ou d'activité physique à des dispositifs conçus pour recueillir et traiter ces informations. Avec le développement croissant des dispositifs de l'IdO, y compris les dispositifs médicaux, le simple fait de porter ou non un dispositif donné peut souvent révéler des informations très sensibles, comme des informations de santé, et par conséquent, il convient de faire preuve de prudence à cet égard.

14. Le retrait du consentement (article 9, paragraphe 3)

En ce qui concerne l'article 9, paragraphe 3 (possibilité de retirer le consentement), le CEPD recommande d'ajouter une référence à l'article 8, paragraphe 1, point b), en plus des références déjà mentionnées à l'article 6.

15. Le caractère «*réalisable*» du consentement exprimé à l'aide des paramètres techniques (article 9, paragraphe 2)

L'article 9, paragraphe 2, dispose que «*... si cela est techniquement possible et réalisable, ... le consentement peut être exprimé à l'aide des paramètres techniques appropriés d'une application logicielle permettant d'accéder à Internet*».

La formulation «*si cela est techniquement possible et réalisable*» manque de clarté. En effet, elle se prête à des interprétations très variées et risque de vider cette obligation de sa substance. L'une des interprétations possibles est que le texte est tout simplement redondant puisqu'il exige que le consentement à l'aide des paramètres techniques soit à la fois « *techniquement réalisable*» et « *techniquement possible*». Une autre interprétation consiste à considérer que la formulation impose une condition supplémentaire d'ordre général (et non technique) concernant le caractère «*réalisable*» du consentement, dont la portée peut être interprétée de manière stricte ou large, et qui pourrait même sans doute inclure des considérations commerciales, comme l'effet d'un consentement exprimé selon ce procédé sur les modèles commerciaux existants et sur les marchés pertinents en général.

Le CEPD recommande donc de remplacer la formulation «*si cela est techniquement possible et réalisable*» par «*si cela est techniquement réalisable*» afin de garantir la sécurité juridique en ce qui concerne la portée de cette obligation[73].

16. L'identification de la ligne appelante (CLI) et le blocage des appels entrants (articles 12 à 14)

La proposition inclut le droit du destinataire d'un appel d'être informé de l'identité de l'appelant et de prendre des mesures à l'encontre des appels, qui empêchent la présentation de leur CLI. Le CEPD se réjouit du maintien de ce droit, compte tenu également du fait qu'il s'agit de l'une des protections permettant aux personnes physiques de prendre des mesures à l'encontre d'émetteurs de communications non sollicitées en violation de la législation applicable.

Pour que le blocage des appels soit un outil efficace pour se protéger des communications non sollicitées, le CEPD recommande en outre que la formulation «*ou présentant un code ou un indicatif spécifique indiquant qu'il s'agit d'un appel commercial, comme prévu à l'article 16, paragraphe 3, point b),*» soit ajoutée après les mots «*bloquer les appels entrants provenant de numéros précis*» à l'article 14, paragraphe 1, point a).

17. Annuaires accessibles au public (article 15)

L'article 15 de la proposition dispose que les «*fournisseurs d'annuaires accessibles au public sont tenus d'obtenir le consentement des utilisateurs finaux qui sont des personnes physiques pour enregistrer dans un annuaire les données à caractère personnel de ces utilisateurs finaux*», tandis que les personnes morales ont le droit de s'y opposer.

Dans l'avis préliminaire, le CEPD a recommandé de maintenir cette disposition et d'en étendre le champ d'application afin qu'elle couvre non seulement les annuaires téléphoniques, mais aussi tous les autres types de services d'annuaires. Par ailleurs, le CEPD a recommandé que l'exigence de consentement pour la «*recherche inversée*» devrait aussi être étendue explicitement à d'autres identifications de services telles que l'adresse électronique ou le nom de l'utilisateur. Nous nous réjouissons des précisions qui ont été apportées à cet effet au considérant 30 et du fait que les téléphones mobiles, les adresses électroniques et les services de renseignements relèvent désormais explicitement du champ d'application de l'article 15.

Nous approuvons néanmoins les recommandations du G29 dans son avis 1/2017, selon lesquelles la proposition devrait indiquer plus clairement qu'un consentement spécifique distinct (c.-à-d. granulaire) est nécessaire pour la recherche et la recherche inversée. Nous recommandons également de supprimer la formulation *«telle qu'elle a été établie par son fournisseur»* de l'article 15, paragraphe 1.

18. Communications non sollicitées (article 16)

Le CEPD se félicite du fait que l'article 16 de la proposition a maintenu, mis à jour et renforcé le mécanisme de protection actuel contre les communications non sollicitées. Les moyens empruntés pour réaliser des communications non sollicitées ont évolué depuis l'entrée en vigueur de la directive «vie privée et communications électroniques». Par exemple, un appel vocal non sollicité peut commencer par un composeur automatique de numéros, diffuser un message enregistré puis utiliser un assistant virtuel pour interagir avec la personne physique appelée au travers d'une série de questions filtres automatisées. L'assistant virtuel peut ensuite utiliser les questions pour transférer la personne physique appelée à un opérateur humain. Ce type d'appel à des fins de prospection directe est désormais traité de la même façon que les appels entièrement automatisés.

Comme le montre cet exemple, le CEPD se réjouit de l'ambition affichée par la proposition d'adopter une approche neutre du point de vue technologique et de moderniser les règles. Le CEPD salue tout particulièrement l'exigence de consentement générale, quelle que soit la technologie utilisée.

Toutefois, des améliorations peuvent encore être apportées à la proposition. Le texte doit être renforcé pour éviter les vides juridiques et pour garantir la sécurité juridique dans les cas limites.

Inquiétudes concernant l'étendue de la protection

L'article 16 de la proposition traite uniquement des *«communications de prospection directe»*. Pour autant, les communications non sollicitées ou malveillantes ne peuvent pas toutes être considérées comme des communications de «*prospection directe*» au sens commercial courant ou au sens de l'article 4, paragraphe 3, point f), qui définit ce terme aux fins du règlement «vie privée et communications électroniques».

Ainsi, par exemple, malgré leur importance, les catégories suivantes de communications non sollicitées semblent ne pas avoir été incluses dans le champ d'application de la protection:

- Certaines communications liées à des tentatives criminelles, par exemple les attaques par hameçonnage et les propositions financières frauduleuses, qui peuvent ne pas toujours être couvertes par la définition de la prospection directe.

- Certains types de communications commerciales, qui peuvent relever ou non de la définition de prospection directe.
- Des communications de nature non commerciale, ou toute autre communication dont il est difficile d'établir s'il s'agit d'une communication de prospection directe (comme, par exemple, certains types de communications envoyées par des partis politiques ou par des organisations religieuses ou caritatives pour demander des dons ou pour assurer la promotion de messages politiques, religieux ou autres[74]).

Pour ces raisons, le CEPD recommande aux législateurs de vérifier s'il est possible d'assurer une protection plus complète pour couvrir tous les types de courriers ou d'appels téléphoniques non sollicités, les messages commerciaux, l'hameçonnage et les autres tentatives malveillantes. À cet effet, le CEPD recommande à la fois d'étendre et de clarifier le champ d'application des «*communications de prospection directe*» et d'introduire des termes supplémentaires comme, par exemple, les «*communications non sollicitées*».

Premièrement, la fourniture d'une protection complète ne peut être assurée en prévoyant simplement des règles spécifiques pour les «*communications de prospection directe*». En effet, avant d'élaborer des règles spécifiques pour les communications de prospection directe, le CEPD recommande d'instaurer une interdiction claire de toutes les communications non sollicitées afin d'éviter des vides juridiques pour un grand nombre de communications non sollicitées malveillantes ou indésirables.

Une autre inquiétude liée au champ d'application concerne la nécessité de mettre en place des règles neutres du point de vue technologique. L'article 16 devrait exiger sans ambiguïté le consentement préalable des destinataires pour tout type de communications électroniques non sollicitées, quels que soient les moyens empruntés (par exemple, courrier électronique, appels vocaux ou vidéo, télécopie, teste, mais aussi messagerie directe via une plateforme (dans le cadre d'un service de la société de l'information). À cet effet, les considérants donnent d'autres exemples.

En outre, le CEPD recommande que les considérants précisent que chaque fois qu'un message de prospection directe est envoyé à une personne physique *travaillant* pour une personne morale, les dispositions applicables aux personnes physiques s'appliqueront[75].

S'agissant des exceptions actuelles concernant les relations existantes et les produits ou services analogues, le CEPD se réjouit du fait que l'article 16, paragraphe 2, de la proposition les ait conservées, mais il recommande que la proposition précise, éventuellement dans un considérant, ce qu'elle entend par «*produits ou services analogues*» et qu'elle explique également la notion de «*relation existante*».

Le retrait du consentement

Le CEPD recommande que l'article 16 précise, d'une part, que le retrait du consentement à la prospection directe est gratuit et, d'autre part, qu'il est aussi simple de retirer que de donner son consentement. Cette précision vise à garantir la cohérence du RGPD[76] et à améliorer la protection des destinataires. Nous constatons que le terme «*gratuit*» est utilisé à l'article 16, paragraphe 2, de la proposition de règlement, mais uniquement en ce qui concerne l'opposition à la prospection directe sur la base des coordonnées obtenues dans le cadre d'une vente.

Garanties pour les appels de prospection directe (article 16, paragraphe 3)

En outre, conformément à l'article 16, paragraphe 3, les personnes physiques ou morales effectuant des appels de prospection directe doivent soit i) présenter l'identité d'une ligne sur laquelle elles peuvent être contactées (article 16, paragraphe 3, point a)), soit ii) présenter un code ou un indicatif spécifique indiquant qu'il s'agit d'un appel commercial (article 16, paragraphe 3, point b)). L'exigence d'un code ou d'un indicatif pour les appels de prospection directe est donc présentée comme une alternative à l'exigence d'identification de la ligne appelante.

Si le CEPD se réjouit de ces deux exigences, il souligne que, pour permettre le retrait effectif du consentement, il est essentiel que les exigences ne soient pas des alternatives, mais plutôt qu'elles soient complémentaires les unes des autres. Ces deux exigences doivent être obligatoires. À cet effet, le mot *«ou»* entre les points a) et b) devrait être remplacé par *«et»*.

Information aux utilisateurs finaux (article 16, paragraphe 6)

Le CEPD craint également que la proposition n'interdise pas explicitement l'utilisation de fausses identités lors de l'envoi de communications de prospection directe. Il est constaté au considérant 34 qu'*«il importe d'interdire l'envoi de messages commerciaux non sollicités à des fins de prospection directe sous une fausse identité, une fausse adresse de réponse ou un faux numéro*». Toutefois, à l'article 16, paragraphe 6, il est simplement affirmé que les utilisateurs finaux sont 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 devrait être complétée, dans une disposition matérielle, par une interdiction claire de l'utilisation d'une fausse adresse de contact à des fins de prospection directe.

Registre européen d'opposition aux appels vocaux

Conformément à l'article 16, paragraphe 4, de la proposition, les États membres peuvent choisir un régime d'opposition aux appels commerciaux vocaux. Le considérant 36 précise en outre que les États membres *devraient être en mesure* de créer et/ou de maintenir des systèmes d'opposition nationaux.

À moins qu'elles ne soient encore améliorées, ces dispositions maintiennent un vide juridique important en ce qui concerne la protection des données à caractère personnel, et elles ne sont pas à la hauteur de l'ambition de créer un cadre juridique plus harmonisé dans toute l'Europe, qui profiterait à la fois aux entreprises et aux personnes physiques. En principe, le CEPD est favorable à un régime de consentement préalable. Néanmoins, pour ceux des États membres qui souhaitent créer ou maintenir leurs propres systèmes, le CEPD recommande aux législateurs de profiter de cette occasion pour créer, à l'échelle européenne, un système d'opposition aux appels de prospection directe non sollicités, en précisant dans le règlement «vie privée et communications électroniques» les modalités du système d'opposition aux appels vocaux à des fins commerciales. Pour les États membres qui choisissent un régime d'opposition aux appels vocaux commerciaux, un dispositif uniforme tel qu'un registre européen d'opposition au démarchage téléphonique pourrait donc représenter un système de référence.

À titre subsidiaire, le règlement devrait au moins exiger clairement que chaque État membre crée un registre national d'opposition au démarchage téléphonique. Il est crucial de mettre un terme aux situations dans lesquelles un utilisateur serait obligé de signifier son opposition

auprès de chaque fournisseur de communications, au lieu simplement de s'inscrire sur une liste d'opposition au démarchage téléphonique.

En outre, le CEPD recommande que le règlement précise que les destinataires d'appels vocaux devraient avoir deux possibilités pour retirer leur consentement: d'une part pour les futurs appels émanant de l'organisation effectuant l'appel (et de toute organisation affiliée à celle-ci) et, d'autre part, la possibilité durant ces appels de s'inscrire sur une liste d'opposition nationale (ou européenne) au démarchage téléphonique.

19. Protéger la sécurité des communications (article 17)

Il est essentiel que le niveau actuel de protection soit maintenu: les législateurs ne devraient pas créer de vide réglementaire en supprimant les obligations de sécurité prévues dans la directive «vie privée et communications électroniques».

Le CEPD se réjouit du fait que la proposition maintienne, à l'article 17, l'obligation imposée par la directive «vie privée et communications électroniques» aux fournisseurs de services d'informer les utilisateurs des services des risques de sécurité détectés, qui doivent être pris en compte lors de l'utilisation du service. En ce qui concerne le destinataire de ces informations, il convient assurément d'informer les utilisateurs finaux (au sens de la définition tirée du CCEE) de ces risques. Toutefois, pour augmenter l'efficacité de l'avertissement de sécurité, il serait souhaitable de préciser que les personne morales utilisant les services doivent être informées ultérieurement. La modification des définitions suggérée à la section 3.1 ci-dessus permettrait d'éclaircir ce point, mais il serait peut-être utile d'ajouter une référence dans le considérant concerné.

Le CEPD admet que les dispositions de la directive «vie privée et communications électroniques» concernant les violations de données ne sont pas nécessaires dans la proposition de règlement, cette question étant couverte par les dispositions correspondantes du RGPD.

Le CEPD est également conscient du fait que les dispositions du CCEE en matière de sécurité et celles de la directive sur les équipements radioélectriques (RED)[77] devraient contribuer à renforcer la sécurité des réseaux, services et terminaux de communications. Par ailleurs, la directive NIS[78] et – dans une moindre mesure – le règlement EIDAS[79] pourraient faire entrer certains des services dans le champ d'application de la proposition de règlement «vie privée et communications électroniques». Cependant, il convient de relever que même le champ d'application global des services couverts par ces différents instruments pourrait ne pas inclure tous les services relevant du champ d'application du règlement «vie privée et communications électroniques». En particulier, comme la portée matérielle du règlement «vie privée et communications électroniques» est plus large que celle de la proposition de CCEE, les obligations de la proposition de CCEE ne s'appliquent pas à tous les services couverts par le règlement «vie privée et communications électroniques». Les exigences de sécurité du RGPD s'appliquent uniquement au traitement de données à caractère personnel, et l'entité responsable est désignée en tant que responsable du traitement ou sous-traitant. Toutefois, il est nécessaire de veiller à la protection de la confidentialité de toutes les données de communications.

Par conséquent, des dispositions particulières sur la sécurité restent également nécessaires dans le règlement «vie privée et communications électroniques» [80]. Le CEPD recommande de préciser dans le règlement «vie privée et communications électroniques» que les obligations en matière de sécurité visées à l'article 40 de la proposition de CCEE devraient s'appliquer *mutatis*

mutandis à tous les services relevant du champ d'application du règlement «vie privée et communications électroniques», indépendamment du fait qu'ils entrent aussi dans le champ d'application de la proposition de CCEE ou non. Cette disposition générale sur la sécurité pourrait être complétée par un considérant énumérant certaines mesures de sécurité supplémentaires concrètes, qui ont été mentionnées dans la consultation publique de la Commission[81] et approuvées par le CEPD dans son avis préliminaire sur le réexamen:

- élaboration de normes minimales de sécurité ou de respect de la vie privée pour les réseaux et services;

- extension des exigences en matière de sécurité afin d'élargir la couverture des logiciels liés à la fourniture d'un service de communication, comme les systèmes d'exploitation embarqués dans des équipements terminaux;

- extension des exigences de sécurité afin d'élargir la couverture de l'internet des objets, tels que ceux utilisés dans les dispositifs informatiques portés sur soi («wearable computing»), la domotique, la communication de véhicule à véhicule, etc.; et

- extension des exigences en matière de sécurité afin d'élargir la couverture de tous les composants de réseau, y compris les cartes SIM, les appareils utilisés pour la commutation ou le routage de signaux, etc.

Ces exigences pourraient faciliter la bonne mise en œuvre des principes de sécurité dès le stade de la conception, de protection des données dès le stade de la conception, et de protection des données par défaut et fourniraient davantage d'orientations aux fabricants et aux fournisseurs de logiciels. En outre, elles pourraient avoir pour effet d'encourager les fabricants des produits, services et applications utilisés dans les services de communications électroniques à prendre en compte les droits au respect de la vie privée et à la protection des données lors de leur développement et de leur conception, à l'instar de ce qui est envisagé au considérant 78 du RGPD.

Chiffrement

Comme le CEPD et le G29 l'ont également relevé dans leurs avis préliminaires, le chiffrement est devenu un outil essentiel pour protéger la confidentialité des communications au sein des réseaux de communications électroniques. Le recours au chiffrement s'est accru après les révélations sur les tentatives d'organisations publiques et privées et de gouvernements d'accéder à des communications[82].

Le CEPD continue de recommander que le règlement «vie privée et communications électroniques» autorise clairement les utilisateurs à recourir au chiffrement de bout en bout (sans «porte dérobée»[83]) pour protéger leurs communications électroniques. Par ailleurs, le CEPD recommande, comme le suggère aussi le G29, d'interdire le déchiffrement, l'ingénierie inverse ou la surveillance des communications protégées par le chiffrement.

En outre, le recours au chiffrement de bout en bout devrait aussi être encouragé et, si nécessaire, rendu obligatoire, conformément au principe de protection des données dès le stade de la conception. Dans ce contexte, le CEPD recommande également à la Commission d'envisager des mesures pour encourager l'élaboration de normes techniques relatives au chiffrement, également en vue d'appuyer les exigences de sécurité revues dans le RGPD.

Le CEPD recommande par ailleurs que le règlement «vie privée et communications électroniques» interdise spécifiquement aux fournisseurs de chiffrement, aux fournisseurs de services de communications et à toute autre organisation (à tous les niveaux de la chaîne d'approvisionnement) d'autoriser ou de faciliter les «portes dérobées».

20 Les voies de recours collectives (article 21)

L'article 21 de la proposition omet toute référence explicite à l'article 80 du RGPD, qui prévoit le droit de la personne concernée de «*mandater un organisme, une organisation ou une association à but non lucratif*», dans certaines conditions, pour qu'il exerce certains droits en son nom, ainsi que la possibilité pour les États membres de prévoir que ces organisations puissent exercer des fonctions similaires, de leur propre initiative, indépendamment de tout mandat confié par une personne concernée. La raison de cette omission n'est pas claire. Pourtant, le règlement «vie privée et communications électroniques» est censé «*préciser et compléter*» le RGPD, qui prévoit plusieurs voies de recours, y compris l'article 80 sur les voies de recours collectives. Le règlement «vie privée et communications électroniques» semble omettre ici un nouveau mécanisme important pour faire respecter les droits des personnes concernées.

L'article 21, paragraphe 2, de la proposition mentionne la possibilité pour les personnes physiques ou morales «*ayant un intérêt légitime*» d'agir en justice, possibilité qui visait peut-être aussi à inclure les voies de recours collectives prévues par le RGPD. L'introduction du concept d'intérêt légitime et l'absence de référence à l'article 80 du RGPD demandent toutefois à être clarifiées. Le CEPD recommande aux législateurs d'ajouter une disposition explicite concernant les voies de recours collectives ou de clarifier la formulation (par exemple en confirmant explicitement l'applicabilité de l'article 80 du RGPD), afin de garantir l'accès aux mécanismes de recours collectifs prévus par le RGPD.

21 Garantir une plus grande harmonisation des amendes (articles 23, paragraphes 4 et 6, et article 24)

Le CEPD se réjouit de l'harmonisation des pouvoirs de contrôle, y compris du niveau des amendes. Une harmonisation accrue des amendes serait toutefois souhaitable. Les articles 23, paragraphes 4 et 6, et 24, de la proposition disposent que les États membres déterminent le régime des sanctions applicables aux violations de certaines dispositions du règlement «vie privée et communications électroniques». Le CEPD est favorable aux recommandations formulées dans l'avis 1/2017 du G29[84], selon lesquelles il serait plus cohérent d'introduire également cette disposition dans le règlement «vie privée et communications électroniques» lui-même.

Notes

[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 (ci-après le règlement «vie privée et communications électroniques»), COM(2017) 10 final, 2017/0003 (COD).

[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 (ci-après la directive «vie privée et communications électroniques»), JO L 201 du 31/7/2002, p. 37, modifiée par la directive 2009/136/CE.

[3] Avis 1/2017 du G29 sur la proposition de règlement relatif à la vie privée et aux communications électroniques (2002/58/CE) (GT247), adopté le 4 avril 2017. Voir également avis 3/2016 du G29 sur l'évaluation et le réexamen de la directive «vie privée et communications électroniques» (2002/58/CE) (GT240), adopté le 19 juillet 2016.

[4] Voir https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-07-22_Opinion_ePrivacy_FR.pdf .

[5] Stratégie pour un marché unique numérique en Europe, communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, 6 mai 2015 (COM(2015) 192 final), disponible à l'adresse suivante: http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52015DC0192&from=FR.

[6] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JO L 281 du 23/11/1995, p. 31.

[7] 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 04/05/2016, p. 1, disponible à l'adresse suivante: http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:L:2016:119:FULL.

[8] Voir avis du G29 1/2017 et 3/2016.

[9] Voir EDRi, *«EDRi's Position on the proposal of an ePrivacy Regulation»*, consultable à l'adresse suivante: <https://edri.org/files/epd-revision/ePR_EDRi_position_20170309.pdf> (document d'orientation, 9 mars 2017) et «*E-Privacy revision: An analysis from civil society groups*» <https://edri.org/files/epd-revision/EDRi_ePrivacyDir-final.pdf> (analyse, 6 juillet 2016).

[10] L'article 7 de la charte protège aussi le droit à la vie privée.

[11] Voir, par exemple, l'article 10 de la Constitution allemande, l'article 37 de la Constitution slovène, l'article 36 de la Constitution croate, l'article 19 de la Constitution grecque, l'article 43 de la Constitution estonienne, l'article 15 de la Constitution italienne, l'article 49 de la Constitution polonaise, l'article 28 de la Constitution roumaine, l'article 72 de la Constitution danoise, l'article 13 de la Constitution néerlandaise, l'article 29 de la Constitution belge, l'article 6, chapitre 2, de la Constitution suédoise, l'article 10 de la Constitution finlandaise, l'article 17 de la Constitution chypriote, l'article 18 de la Constitution espagnole, les articles 10 et 10a de la Constitution autrichienne, l'article 13 de la Constitution tchèque et l'article 22 de la Constitution slovaque.

[12] L'article 8, paragraphe 1, point b), de la proposition exige notamment le consentement pour *«l'utilisation des capacités de traitement et de stockage des équipements terminaux et la collecte d'informations provenant des équipements terminaux des utilisateurs finaux»*. Par ailleurs, l'article 6, paragraphe 2, point c), et paragraphe 3, impose l'obligation d'obtenir le consentement pour le traitement de contenu et de métadonnées. En outre, l'article 16 sur les communications non sollicitées exige, généralement sous réserve de certaines exceptions, que le consentement préalable constitue la base juridique des communications de prospection directe.

[13] Voir l'article 1er et le considérant 14 du RGPD concernant les personnes morales, desquels il ressort que le RGPD ne reconnaît qu'aux personnes physiques, et non aux personnes morales, le droit à la protection des données à caractère personnel.

[14] Sans protection de la confidentialité, il serait impossible d'utiliser les communications électroniques pour de nombreuses opérations commerciales et pour les échanges au sein de l'administration publique. En outre, les organisations gagnent aussi à être protégées des appels téléphoniques non sollicités, qu'ils soient destinés à des salariés spécifiques ou à un standard central. De même, les personnes morales ont le droit de bloquer les appels entrants en ce qui concerne non seulement les appels destinés à des salariés individuels, mais aussi les numéros de téléphone généraux utilisés par l'organisation.

[15] Une plus grande harmonisation des amendes serait toutefois souhaitable. Voir section 21 de l'annexe pour plus d'informations.

[16] À proprement parler, le VoIP est une famille de protocoles qui permet la fourniture de services de téléphonie sur des réseaux au moyen de protocoles internet (principalement IP) au lieu des normes de la téléphonie traditionnelle. Ces technologies sont utilisées par des fournisseurs de services dits «par contournement», mais aussi par des fournisseurs de réseaux traditionnels. Dans un contexte réglementaire, le terme «*VoIP*» est souvent utilisé comme un synonyme de téléphonie par l'internet fourni en plus des réseaux de transmission de base. Telle est la signification retenue dans le présent avis.

[17] L'article 2, paragraphe 1, de la proposition dispose que le règlement «vie privée et communications électroniques» s'applique au «*traitement des données de communications électroniques effectué en relation avec la fourniture et l'utilisation de services de communications électroniques dans l'Union et aux informations liées aux équipements terminaux des utilisateurs finaux*».

[18] Des clarifications supplémentaires recommandées par le CEPD sont exposées au chapitre 1 de l'annexe.

[19] Proposition de directive du Parlement européen et du Conseil établissant le code des communications électroniques européen, COM (2016) 590 final/2, 2016/0288(COD) du 12/10/2016.

[20] Directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive «cadre»), telle que modifiée.

[21] La proposition de CCEE repose uniquement sur l'article 114 TFUE puisqu'il vise à instaurer le marché interne des communications électroniques et à en garantir le bon fonctionnement. En revanche, la proposition «vie privée et communications électroniques» se fonde sur une double base juridique: l'article 16 TFUE, la même base juridique spécifique que celle du RGPD, ainsi que l'article 114 TFUE. L'article 16 TFUE seul aurait été insuffisant car les nouvelles dispositions non seulement «*préciseront*» certaines dispositions du RGPD, mais elles les «*compléteront*» par des dispositions qui ne se limitent pas à la protection des données à caractère personnel.

[22] Le terme «*abonné*» (précédemment utilisé dans l'actuelle directive «vie privée et communications électroniques») n'est plus utilisé. Il est également utile de comparer la proposition de nouvelle définition à l'article 2, point a), de l'actuelle directive «vie privée et communications électroniques», qui définit un «*utilisateur*» comme «*toute personne physique utilisant un service de communications électroniques accessible au public à des fins privées ou professionnelles sans être nécessairement abonnée à ce service*».

[23] Pour une discussion plus détaillée, voir également page 26, paragraphe 40, point c), de l'avis 1/2017 du G29.

[24] Voir, par exemple, l'évaluation des choix scientifiques et technologiques (STOA), Parlement européen, *Potential and impacts of cloud computing services and social network websites*, 2014. PE 513.546. Disponible à l'adresse suivante: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/513546/IPOL-JOIN_ET(2014)513546_EN.pdf

[25] Voir avis 1/2017 du G29, paragraphe 40, point c).

[26] Dans ce contexte, il est utile de rappeler l'article 2, point a), de la directive «vie privée et communications électroniques», qui définit actuellement un «*utilisateur*» comme «*toute personne physique utilisant un service de communications électroniques accessible au public à des fins privées ou professionnelles sans être nécessairement abonnée à ce service*».

[27] Le CEPD recommande aux législateurs d'étudier attentivement la meilleure façon de garantir des exceptions appropriées et adaptées pour couvrir ces situations. Voir également, à cet égard, point 18, tiret 4, de l'avis 1/2017 du G29, qui recommande d'instaurer une exception qui soit fondée sur la notion d'«*exception domestique*» au titre du RGPD, mais qui intègre également une utilisation professionnelle limitée pour les fonctionnalités ordinaires telles que la recherche par mots clés.

[28] Cette affirmation repose sur l'hypothèse que la définition d'«*utilisateur final*» est modifiée comme indiqué aux sections 3.1 et 3.2 ou remplacée par un autre terme défini de manière plus appropriée. Le CEPD relève également que la notion de «*concerné(e)*» devrait être évitée dans la mesure où elle crée des incertitudes supplémentaires inutiles en ce qui concerne l'identité de la personne qui devrait donner son consentement.

[29] Comme il est expliqué à la section 3.1 concernant les définitions, pour les besoins de certaines dispositions, notamment en ce qui concerne les annuaires accessibles au public visés à l'article 15, un autre terme sera plus approprié pour s'assurer que les personnes abonnées au service seront en mesure de décider.

[30] En effet, dans les communications quotidiennes, les personnes physiques partagent souvent des données à caractère personnel de tiers, à des fins privées mais aussi professionnelles. Certaines de ces données à caractère personnel, comme, par exemple, les informations personnelles ou intimes communiquées à des parents ou à des amis proches, ou le contenu des communications échangées entre des médecins, des avocats, des enquêteurs spécialisés dans les fraudes, etc., peuvent être particulièrement sensibles.

[31] Voir également la recommandation formulée au point 18 de l'avis 1/2017 du G29, qui suggère de préciser que le traitement des données de personnes autres que les utilisateurs finaux concernés (par exemple, l'image ou la description d'un tiers dans un échange entre deux personnes) doit également respecter toutes les dispositions pertinentes du RGPD.

[32] Le CEPD note également que le RGPD concerne la protection des données à caractère personnel, qui constitue un droit distinct, énoncé dans un article différent, à savoir l'article 8 de la charte. Par ailleurs, le fondement juridique des deux instruments n'est pas non plus identique. Enfin, la couverture des personnes protégées est

différente, étant donné que la directive «vie privée et communications électroniques» prévoit aussi la protection des personnes morales. En outre, alors qu'il aurait été possible d'inclure de nombreuses dispositions de la directive «vie privée et communications électroniques» dans le RGPD lui-même, cela n'a pas été le cas. Le considérant 173 et l'article 95 du RGPD appellent à clarifier la relation entre les deux instruments juridiques dans le nouvel instrument législatif en matière de vie privée et de communications électroniques.

[33] Voir également point 21, page 16, de l'avis 1/2017 du G29.

[34] Un phénomène semblable est également observé dans le secteur des applications mobiles, qui demandent souvent l'autorisation d'accéder aux différentes capacités et fonctions d'un téléphone mobile, sans que celles-ci soient nécessaires au fonctionnement de l'application ou à la fourniture du service, notamment l'accès au Wifi, au GPS, à l'appareil photo, aux messages, aux contacts, à l'historique de navigation ou aux images. On pourrait citer comme exemple l'application «lampe torche», dont la fonctionnalité est de fournir une lumière très vive, mais qui demande un accès démesuré à un très grand nombre des catégories de données susmentionnées alors que, de toute évidence, elles ne sont pas nécessaires au fonctionnement du service fourni.

[35] Dans le considérant 42 du RGPD, il est souligné que «*[l]e consentement ne devrait pas être considéré comme ayant été donné librement si la personne concernée ne dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice*». L'attention est également attirée sur le fait qu'«*une déclaration de consentement rédigée préalablement par le responsable du traitement [...] ne devrait contenir aucune clause abusive*». Par ailleurs, le considérant 43 énonce que «*[p]our garantir que le consentement est donné librement, il convient que celui-ci ne constitue pas un fondement juridique valable pour le traitement de données à caractère personnel dans un cas particulier lorsqu'il existe un déséquilibre manifeste entre la personne concernée et le responsable du traitement*». Le même considérant 43 prévoit que «*[l]e consentement est présumé ne pas avoir été donné librement [...] si l'exécution d'un contrat, y compris la prestation d'un service, est subordonnée au consentement malgré que celui-ci ne soit pas nécessaire à une telle exécution*». Ce dernier point est réaffirmé à l'article 7, paragraphe 4, du RGPD, qui dispose qu'«*[a]u moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat*».

[36] Avis nº 7/2015 du CEPD: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_FR.pdf.

[37] En ce qui concerne les possibilités de nouveaux modèles commerciaux innovants et respectueux des lois de l'UE en matière de protection des données, voir, par exemple, l'avis nº 9/2016 du CEPD sur les systèmes de gestion des informations personnelles («PIMS») intitulé «*Vers une plus grande autonomie des utilisateurs dans la gestion et le traitement des données à caractère personnel*».

[38] Une enquête Eurobaromètre récente a révélé que près de 90% des citoyens de l'UE sont effectivement favorables à de tels paramètres par défaut respectueux de la vie privée. *TNS Political & Social, à la demande de la Commission européenne, «Flash Eurobarometer 443 - July 2016, "e-Privacy" Report, EN»* (décembre 2016), p. 43.

[39] Voir page 16, sous l'intitulé *«Mécanismes pour donner et retirer le consentement»*.

[40] S'agissant de la définition des utilisateurs finaux, voir la recommandation formulée aux sections 3.1 et 3.2.

[41] Des recherches menées par des membres de l'EDRi montrent que la plupart des services actuels basés sur des métadonnées de localisation seraient fondés non pas sur le consentement, mais sur l'anonymisation. Les chercheurs ont exprimé des inquiétudes quant au fait que les données ne seraient, en réalité, pas entièrement rendues anonymes. https://www.openrightsgroup.org/ourwork/reports/mobile-data.

[42] En ce qui concerne la possibilité de prévoir de telles exceptions, voir également la section 3.3 ci-dessus, qui traite de la relation entre le RGPD et le règlement «vie privée et communications électroniques».

[43] Concernant la notion de séparation fonctionnelle et les mesures organisationnelles et techniques qui peuvent être prises pour en garantir la mise en œuvre, voir également section III.2.3, pages 28 à 33 de l'avis 3/2013 du G29 sur la limitation des finalités (GT203), adopté le 2 avril 2013.

[44] Affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland*, EU:C:2014:238.

[45] Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, OJ L 105, 13/5/2006, p. 54.

[46] Affaires jointes C-203/15 et C-698/15, *Tele2 Sverige AB et Watson*, EU:C:2016:970.

[47] Voir, par analogie, C-275/06, *Promusicae/Telefónica de España SAU*, EU:C:2007:454, conclusions de l'avocat général J. Kokott, points 86 à 88.

[48] Voir également CEPD, *Assessing the necessity of measures that limit the fundamental rights to the protection of personal data: A "Toolkit"* [Évaluer la nécessité de mesures limitant les droits fondamentaux à la protection des données à caractère personnel: une «boîte à outils»], 11 avril 2011, disponible à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf.

[49] Voir également point 11 de l'avis de l'Académie européenne pour la liberté de l'information et la protection des données (EAID), 21 mars 2017, disponible à l'adresse suivante: www.eaid-berlin.de/wp-content/uploads/2017/04/EAID_Opinion_E-Privacy-Regulation.pdf (EAID Opinion).
[50] Voir, par exemple, l'avis du CEPD sur les propositions de la Commission de règlement du Parlement européen et du Conseil sur les opérations d'initiés et les manipulations de marché, et de directive du Parlement européen et du Conseil relative aux sanctions pénales applicables aux opérations d'initiés et aux manipulations de marché, adopté le 10 février 2012 (2012/C 177/01), section 2.3.2, en particulier, points 27 et 28, disponible à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/12-02-10_market_manipulation_en.pdf.
[51] Voir l'article 48 du RGPD «*Transferts de divulgations non autorisées par le droit de l'Union*».
[52] Voir avis préliminaire du CEPD, section X.3, p. 21.
[53] Proposition de directive du Parlement européen et du Conseil établissant le code des communications électroniques européen, COM (2016) 590 final/2, 2016/0288(COD) du 12/10/2016.
[54] Ces observations s'inscrivent dans le droit fil de celles formulées précédemment par le CEPD à ce sujet dès 2008 et 2009. Ainsi, à l'occasion du dernier réexamen de la directive «vie privée et communications électroniques» en 2009, le CEPD a rendu deux avis à deux stades différents de la procédure législative. Dans son premier avis, le CEPD a fait valoir que «*l'importance croissante des réseaux mixtes (privés/publics) et des réseaux privés dans la vie quotidienne, et le risque accru qui en découle pour les données à caractère personnel et la vie privée, justifient la nécessité d'appliquer à ces services les mêmes règles que celles qui s'appliquent déjà aux services de communications électroniques publics. À cet effet, le CEPD estime qu'il convient de modifier la directive afin d'en étendre le champ d'application à ce type de services privés [...]*».
Dans son deuxième avis, rendu à un stade ultérieur de la procédure législative, lors de la discussion portant sur des amendements spécifiques, le CEPD a suggéré d'inclure dans le champ d'application de la directive «vie privée et communications électroniques» au moins «*le traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux de communications publics et privés ou* ***sur les réseaux privés accessibles au public*** *dans la Communauté*» (caractères gras ajoutés).
Avis du contrôleur européen de la protection des données du 10 avril 2008 sur la proposition de directive du Parlement européen et du Conseil modifiant, entre autres, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive «vie privée et communications électroniques»), rendu le 10 avril 2008 (2008/C 181/01), disponible à l'adresse suivante: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2008/08-04-10_e-privacy_FR.pdf Voir en particulier les points 22 à 24. Voir également le deuxième avis du contrôleur européen de la protection des données du 9 janvier 2009 relatif au réexamen de la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive «vie privée et communications électroniques»), rendu le 9 janvier 2009 (2009/C 128/04), disponible à l'adresse suivante: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2009/09-01-09_ePricacy_2_FR.pdf Voir en particulier les points 60 à 72, et notamment la citation tirée du point 66.
[55] CEPD, avis 4/2017 sur la proposition de directive concernant certains aspects des contrats de fourniture de contenu numérique, 14 mars 2017.
[56] Voir également *«EDRi's Position on the proposal of an ePrivacy Regulation»* (document d'orientation, 9 mars 2017).
[57] Voir avis 1/2017 du G29, paragraphe 40, point g).
[58] L'article 2, paragraphe 4, de la proposition de CCEE définit les «*services de communications électroniques*» en faisant référence, entre autres, aux *«services de communications interpersonnelles»*, qui sont à leur tour définis à l'article 2, paragraphe 5, de la proposition de CCEE.
[59] Voir également l'annexe, section 18, qui traite des inquiétudes relatives à la portée de la protection contre les communications non sollicitées.
[60] Voir également paragraphe 2, deuxième phrase, de l'avis de l'EAID.
[61] Pour une justification et une vue d'ensemble plus détaillées, voir l'avis 1/2017 du G29, paragraphes 18 et 26.
[62] Avis 2/2006 du G29 sur les problèmes de protection de la vie privée liés à la fourniture de services de filtrage du courrier électronique (GT118), adopté le 21 février 2006.
[63] Pour des informations générales sur la technologie, voir les pages https://fr.wikipedia.org/wiki/Modèle_OSI concernant le modèle OSI et https://fr.wikipedia.org/wiki/Suite_des_protocoles_Internet concernant la suite des protocoles internet.
[64] Michael Hayden, ancien directeur de la CIA et de la NSA, avait déclaré en avril 2014, à l'université John Hopkins: «*Nous tuons nos cibles grâce aux métadonnées*». Voir: Pomerantz, J., Metadata, United States of America: MIT Press 2015, p. 118. Le discours prononcé à l'université John Hopkins est disponible à l'adresse suivante:

https://www.youtube.com/watch?v=kV2HDM86XgI – les propos de M. Hayden cités ici sont tenus à 17:59 minutes.

[65] Les métadonnées utilisées lors de l'enquête pénale avaient conduit à l'arrestation des assassins présumés de l'ancien Premier ministre Rafiq Hariri. «*Sur les 10 téléphones portables utilisés avec ces 10 cartes téléphoniques, il a été établi que 5 venaient d'un magasin à Tripoli*». Conseil de sécurité des Nations unies, Rapport de la Commission d'enquête internationale indépendante créée par la résolution 1595 (2005) du Conseil de sécurité, S2005/662, Beyrouth: 19 octobre 2005, nº 151, p. 147, disponible à l'adresse suivante: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/563/67/PDF/N0556367.pdf?OpenElement.

[66] De Montjoye, Y. A., Hidalgo, C. A., Verleysen, M., & Blondel, V. D. (2013), *Unique in the Crowd: The privacy bounds of human mobility*, Nature SRep, 3, disponible à l'adresse suivante: http://www.nature.com/articles/srep01376. D'après cette étude, quatre points spatio-temporels sont suffisants pour identifier de manière unique 95% des personnes physiques.

[67] New York Times Editorial Board, Surveillance: *A Threat to Democracy*, 11 juin 2013, disponible à l'adresse suivante: http://www.nytimes.com/2013/06/12/opinion/surveillance-a-threat-to-democracy.html?hp.

[68] Voir avis 1/2017 du G29, point 18, ainsi que les points 10, 33 et 46 sur les métadonnées.

[69] Avis préliminaire du CEPD, pages 16 et 17.

[70] Le texte législatif devrait faire apparaître clairement que lorsqu'une organisation a recours aux services d'analyse d'un tiers, qui fixe ses propres témoins de connexion, ceux-ci ne peuvent être considérés comme des témoins d'origine.

[71] Avis du G29 nº 04/2012 sur l'exemption de l'obligation de consentement pour certains cookies (WP194), disponible à l'adresse suivante: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_fr.pdf.

[72] Pour plus de recommandations, voir également l'avis 1/2017 du G29, pages 18 et 19, point 25.

[73] Voir également le point 7 de l'avis de l'EAID.

[74] Le considérant 32 relatif aux messages assurant la promotion de partis politiques ou invitant à soutenir les objectifs d'une organisation à but non lucratif, va dans le bon sens, mais il est insuffisant pour garantir la sécurité juridique d'une manière complète et dans toutes les situations concernées. Comme il s'agit d'un domaine où il peut s'avérer nécessaire de trouver un juste équilibre entre la liberté d'expression et le droit au respect de la vie privée, d'autres orientations seraient particulièrement utiles.

[75] Voir également avis 1/2017 du G29, paragraphe 43, point c).

[76] L'article 7, paragraphe 3, du RGPD exige notamment qu'il doit être aussi simple de retirer que de donner son consentement et que les personnes physiques devraient avoir le droit de retirer leur consentement à tout moment.

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

[78] 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.

[79] Règlement (EU) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE , JO L 257, 28.8.2014, p. 73

[80] Cela étant, le RGPD et le règlement «vie privée et communications électroniques» devraient être harmonisés de manière à assurer la cohérence. Par exemple, le CEPD recommande de faire un renvoi aux obligations de sécurité prévues par le RGPD (y compris les évaluations et l'obligation de rendre compte des incidences sur la protection des données).

[81] Voir la question 21 du questionnaire de la consultation publique.

[82] Avis préliminaire du CEPD, p. 19; avis 3/2016 du G29, p. 19.

[83] Voir https://fr.wikipedia.org/wiki/Porte_dérobée.

[84] Voir point 38 de l'avis 1/2017 du G29.