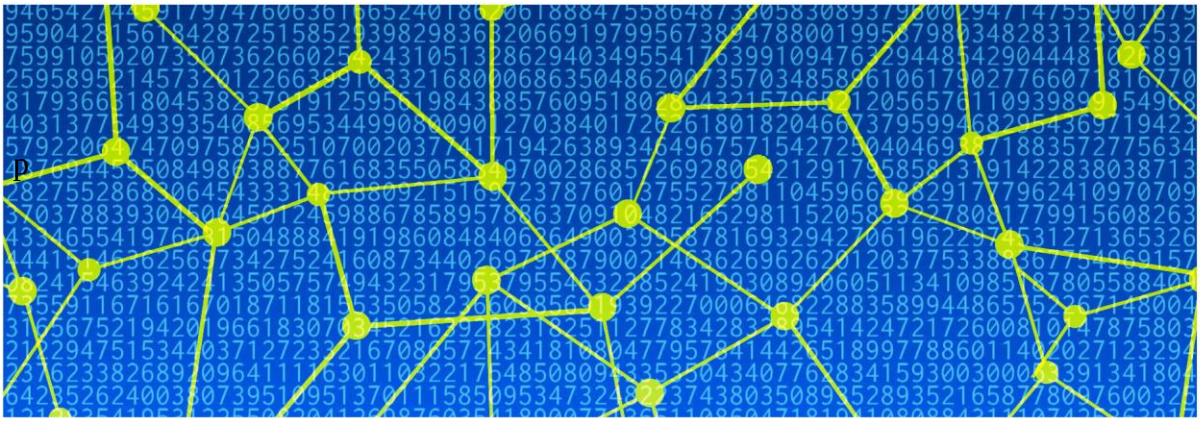

EUROPEAN DATA PROTECTION SUPERVISOR

Avis 5/2016

Avis préliminaire du CEPD sur le réexamen de la directive «vie privée et communications électroniques» (directive 2002/58/CE)

22 juillet 2016

Le contrôleur européen de la protection des données (CEPD) est une institution indépendante de l'Union européenne 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'être constructifs et proactifs. 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 se rapporte à la mission du CEPD de conseil des institutions de l'Union sur les implications de leurs politiques en matière de protection des données et de promotion d'une élaboration responsable des politiques, conformément à l'action nº 9 de la stratégie du CEPD: «Faciliter l'élaboration responsable et éclairée de politiques».

Synthèse

Le présent avis expose, à la demande de la Commission européenne, la position du CEPD sur les questions clés liées au réexamen de la directive 2002/58/CE (directive «vie privée et communications électroniques»)[1].

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: une plus grande clarté, mais aussi une meilleure application des règles sont nécessaires. Nous en avons besoin pour garantir la confidentialité de nos communications, un droit fondamental inscrit à l'article 7 de la charte des droits fondamentaux de l'Union européenne. En outre, nous avons besoin de dispositions pour compléter et, le cas échéant, préciser les protections offertes par le règlement général sur la protection des données (RGPD). Par ailleurs, nous devons également maintenir le niveau élevé de protection dont nous disposons actuellement, lorsque la directive «vie privée et communications électroniques» prévoit des garanties plus spécifiques que le RGPD. Les définitions du RGPD, son champ d'application territorial, les mécanismes de coopération entre les autorités chargées de son application et les mécanismes de cohérence, ainsi que la possibilité de prévoir une certaine flexibilité et des orientations devraient être retenus dans le domaine de la vie privée et des communications électroniques.

Le champ d'application du nouveau cadre juridique doit être élargi. Il s'agit de tenir compte des évolutions technologiques et sociétales et de garantir que les personnes physiques bénéficient du même niveau de protection pour l'ensemble des services équivalents sur le plan fonctionnel, qu'ils soient fournis, par exemple, par des compagnies de téléphone traditionnelles, des services de voix sur IP ou des applications de messagerie sur téléphone mobile. Il est en effet nécessaire d'aller encore plus loin et de protéger non seulement les services «équivalents sur le plan fonctionnel», mais aussi les services qui offrent de nouvelles possibilités de communication. Les nouvelles règles devraient également continuer à s'appliquer sans ambiguïté aux communications de machine à machine dans le contexte de l'internet des objets, quel que soit le type de réseau ou de service de communications utilisé. Elles devraient aussi garantir que la confidentialité des communications des utilisateurs sera protégée sur tous les réseaux accessibles au public, notamment les services de Wifi dans les hôtels, les cafés, les magasins, les aéroports et les réseaux offerts par les hôpitaux aux patients et par les universités aux étudiants, ainsi que les endroits névralgiques créés par les administrations publiques.

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 de témoins de connexion (cookies)». Hormis une série d'exceptions bien définies (comme l'analytique d'origine), aucune communication ne devrait faire l'objet d'un traçage et d'une surveillance sans consentement librement donné, que ce soit à l'aide de témoins de connexion, d'une capture d'empreintes numériques ou d'autres moyens technologiques. Les utilisateurs doivent également avoir accès à des mécanismes efficaces et faciles à utiliser pour donner et retirer leur consentement dans le navigateur (ou un autre logiciel ou le système d'exploitation).

Afin de mieux protéger la confidentialité des communications électroniques, l'exigence actuelle de consentement pour les données relatives au trafic et les données de localisation doit elle aussi être maintenue et renforcée. La portée de cette disposition devrait être élargie afin de couvrir toute personne et pas uniquement les compagnies de téléphone traditionnelles et les fournisseurs d'accès à l'internet.

Les nouvelles règles devraient également autoriser clairement les utilisateurs à recourir au chiffrement de bout en bout (sans «porte dérobée») pour protéger leurs communications électroniques. Le déchiffrement, l'ingénierie inverse ou la surveillance de communications protégées par le chiffrement devraient être interdits.

Enfin, les nouvelles règles en matière de vie privée et de communications électroniques devraient offrir une protection contre les communications non sollicitées. Il convient de les actualiser et de les renforcer en exigeant le consentement préalable des destinataires pour tous les types de communications électroniques non sollicitées, quels que soient les moyens empruntés.

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,

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:

I. 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 le réexamen de la directive «vie privée et communications électroniques»[2].

La consultation du CEPD a eu lieu parallèlement à la consultation publique organisée par la Commission, qui s'est clôturée le 5 juillet 2016[3]. La Commission a également sollicité l'avis du groupe de travail «Article 29» sur la protection des données (GT29), auquel le CEPD a contribué en tant que membre à part entière[4].

Le présent avis contient la position préliminaire du CEPD sur le réexamen de la directive «vie privée et communications électroniques», qui porte plus particulièrement sur les questions pour lesquelles son avis a été expressément demandé par la Commission. L'avis constitue aussi la contribution du CEPD à la consultation publique et, en tant que tel, il peut également aborder des questions qui n'ont pas été explicitement soulevées par la Commission dans sa demande d'avis. Le CEPD est également susceptible de donner son avis aux stades ultérieurs de la procédure législative.

Le réexamen de la directive «vie privée et communications électroniques» 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.

Le réexamen 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. La directive «vie privée et communications électroniques» énonce des règles spécifiques, essentiellement dans le but de garantir la confidentialité et la sécurité des communications électroniques. Elle protège aussi les intérêts légitimes des abonnés qui sont des personnes morales.

II. NÉCESSITÉ D'UN NOUVEL INSTRUMENT JURIDIQUE EN MATIÈRE DE VIE PRIVÉE ET DE COMMUNICATIONS ÉLECTRONIQUES

Le CEPD soutient l'initiative de la Commission de moderniser, d'actualiser et de renforcer les dispositions de la directive «vie privée et communications électroniques». Il partage le point de vue également exprimé par le GT29 dans son récent avis[8], ainsi que par certains groupes de la société civile dans leur analyse commune 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 croit également que des dispositions législatives sélectives et ciblées sont nécessaires pour garantir une protection solide, intelligente et efficace.

La directive «vie privée et communications électroniques» actuelle fournit une protection dans des domaines qui ne sont pas couverts par la notion de traitement de données à caractère personnel, condition à l'applicabilité des instruments de base en la matière tels que la directive 95/46/CE ou le RGPD. Elle prévoit des règles plus précises dans certaines situations de traitement, lorsque les répercussions potentielles du traitement sont importantes. En outre, elle s'intéresse aux actions pour lesquelles le traitement de données à caractère personnel n'est pas nécessairement la principale source d'inquiétude pour la personne physique, par exemple la transmission de messages non sollicités.

II.1 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 directive «vie privée et communications électroniques» est le seul instrument du droit dérivé de l'Union européenne mettant pleinement en œuvre l'article 7 de la charte.

Par ailleurs, la directive ne se borne pas à mettre en œuvre l'article 7 et à préciser les règles en matière de protection des données pour un secteur économique particulier. Elle protège aussi les intérêts légitimes des personnes morales concernant la confidentialité des communications. Au vu des récentes évolutions, et notamment du volume sans cesse croissant de communications électroniques, de la surveillance accrue de ces communications par des entités publiques et privées, et des nouvelles avancées technologiques telles que l'informatique en nuage, l'internet des choses et les données massives, il est de plus en plus important de protéger la confidentialité des communications.

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, les opérations pourraient uniquement être effectuées de personne à personne. La directive «vie privée et communications électroniques» impose à tous les fournisseurs de communications électroniques d'être des messagers dignes de

confiance et affranchit les personnes physiques et les organisations de la nécessité de déterminer s'ils peuvent ou non s'en remettre à un fournisseur donné pour les services de communications. Cette obligation devrait continuer à s'appliquer, comme c'est le cas aujourd'hui, à l'ensemble des communications, quels qu'en soient l'expéditeur, le destinataire et le contenu. En effet, le contenu d'une communication devrait normalement échapper au fournisseur de communications.

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 du droit dérivé de l'Union qui fixe les normes juridiques spécifiques nécessaires (sur la relation entre le RGPD et l'instrument futur en matière de vie privée et de communications électroniques, voir la section III.2 ci-dessous).

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] et ils se sont généralement dotés d'un corpus législatif distinct en la matière. Étant donné l'existence de règles nationales, de nouvelles dispositions, davantage harmonisées au niveau de l'Union européenne, contribuent à renforcer la sécurité juridique. El tant que telles, elles apportent un meilleur bénéfice 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 juridictions.

II.2 Le niveau actuel de protection ne doit pas être réduit

En outre, nous avons besoin de nouvelles dispositions en matière de vie privée et de communications électroniques pour maintenir le niveau de protection élevé des données à caractère personnel dont nous disposons actuellement, lorsque la directive «vie privée et communications électroniques» prévoit des garanties plus spécifiques que celles prévues dans le RGPD.

Par exemple, alors que le RGPD ne définit pas spécifiquement les fondements juridiques possibles du traitement qui peuvent être autorisés dans telle ou telle situation, la directive «vie privée et communications électroniques» est plus précise dans certains contextes spécifiques en imposant le consentement en tant que base juridique. Par exemple, l'article 5, paragraphe 3, de la directive impose le consentement en cas de stockage ou d'accès à des informations stockées dans un équipement terminal (la règle dite «du témoin de connexion»). Par ailleurs, l'article 6, paragraphe 3, exige le consentement pour l'utilisation de données relatives au trafic à des fins de commercialisation ou de fourniture de services à valeur ajoutée. En outre, l'article 13 sur les communications non sollicitées exige également que le consentement préalable soit le fondement juridique de certains types de communications à certaines conditions.

Par ailleurs, la directive «vie privée et communications électroniques» protège aussi les personnes morales concernant les communications non sollicitées ainsi que d'autres aspects liés

à leur rôle d'abonné à des services de communications électroniques. Le RGPD ne couvre pas ces besoins[12].

II.3 Des règles précises dans certaines circonstances

La directive «vie privée et communications électroniques» prévoit 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 promotionnelles.

En principe, la directive «vie privée et communications électroniques» aborde ce genre de situations sans exiger d'analyse aux conditions du RGPD. Toutefois, les dispositions de la directive ont elles-mêmes fait l'objet d'interprétations diverses. Le nouvel instrument devrait par conséquent être l'occasion de clarifier certains termes ou concepts.

III. QUESTIONS LIÉES AU FONDEMENT JURIDIQUE

III.1 Fondement juridique du nouvel instrument juridique en matière de vie privée et de communications électroniques

Le CEPD recommande à la Commission d'envisager un double fondement juridique pour le nouvel instrument juridique en matière de vie privée et de communications électroniques. L'un d'eux devrait être l'article 16 du traité sur le fonctionnement de l'Union européenne (ci-après «TFUE»). Il s'agit là du même fondement juridique que pour le RGPD. Le second devrait être le fondement juridique actuel de la directive «vie privée et communications électroniques», soit l'article 114 du TFUE sur le rapprochement des législations (ancien article 95 du traité CE).

Il ne serait pas suffisant de retenir l'article 16 du TFUE comme seul fondement juridique, étant donné que non seulement les nouvelles dispositions «préciseront» certaines dispositions du RGPD, mais aussi qu'elles les «compléteront» aussi par des dispositions qui ne se limitent pas à la protection des données à caractère personnel (voir également la section II sur la *nécessité d'un nouvel instrument juridique en matière de vie privée et de communications électroniques* et la section III.2 sur la *relation entre le RGPD et le nouvel instrument juridique en matière de vie privée et de communications électroniques*).

III.2 Relation entre le RGPD et les nouvelles dispositions en matière de vie privée et de communications électroniques

Le CEPD recommande que le RGPD et les nouvelles dispositions en matière de vie privée et de communications électroniques continuent à se compléter comme c'est le cas actuellement. Les termes actuels «*complètent et précisent*» sont satisfaisants pour définir cette relation. Pour une plus grande clarté, le CEPD recommande de préciser dans un considérant que les nouvelles dispositions en matière de vie privée et de communications électroniques sont «sans préjudice» des dispositions actuelles du RGPD. Autrement dit, les nouvelles dispositions en matière de vie privée et de communications électroniques ne devraient pas créer de dérogations supplémentaires aux règles du RGPD.

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 (voir la section III.1) 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.

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 appellent à clarifier la relation entre les deux instruments juridiques dans le nouvel instrument législatif en matière de vie privée et de communications électroniques.

III.3 Un règlement plutôt qu'une directive

Bien que les objectifs du réexamen puissent être aussi atteints par une directive, le CEPD recommande aux législateurs de donner au nouvel instrument juridique la forme d'un règlement plutôt que d'une directive. Ce choix présenterait les avantages suivants:

- il serait plus cohérent avec l'approche adoptée dans le RGPD;
- il assurerait un niveau de protection plus cohérent et égal pour les personnes physiques et les autres entités protégées par ses dispositions;
- par ailleurs, il contribuerait à assurer des conditions de concurrence équitables aux organisations qui doivent se conformer à ses dispositions et réduirait leurs coûts de mise en conformité;
- enfin, un règlement permettrait de mieux tirer parti du mécanisme de guichet unique ainsi que des mécanismes de coopération et de cohérence offerts par le RGPD.

Cela étant, il ne peut être exclu que, dans certaines situations, il est parfois nécessaire de fournir une certaine marge de manœuvre aux États membres. Cet objectif peut être atteint quel que soit le type d'instrument juridique retenu.

Le CEPD recommande de limiter au strict nécessaire toute possibilité de législation nationale divergente. Enfin, il recommande que le nouvel instrument juridique indique clairement que toute règle nationale divergente, et en particulier toute dérogation (comme celles visées à l'article 15 actuel), respecte pleinement les dispositions de la charte.

Le choix d'un règlement permettrait aussi d'utiliser plus facilement, dans le domaine de la vie privée et des communications électroniques, le nouveau cadre de protection des données créé par le RGPD ainsi que sa boîte à outils solide et efficace (pour ce qui est, par exemple, des définitions, du champ d'application et des mécanismes de contrôle), de manière à garantir la sécurité juridique et la cohérence. Les définitions du RGPD, son champ d'application territorial, les mécanismes de coopération entre les autorités chargées de son application et les mécanismes de cohérence, ainsi que la possibilité de prévoir une certaine flexibilité et des orientations devraient être retenus dans le domaine de la vie privée et des communications électroniques.

Sous sa forme la plus complète, cet objectif pourrait être atteint en intégrant le plus grand nombre possible de nouvelles dispositions dans le RGPD, à condition que cela soit concevable sans remettre en cause l'équilibre des intérêts voulu par les législateurs. Dans ce cas, les

nouvelles dispositions en matière de vie privée et de communications électroniques pourraient offrir aux responsables du traitement et aux personnes physiques un cadre horizontal plus simple en matière de vie privée et de protection des données dans le même RGPD. Même si cette option n'est pas disponible, les nouvelles dispositions devraient garantir que le cadre du RGPD peut être pleinement utilisé pour les nouvelles dispositions en matière de vie privée et de communications électroniques. En tout état de cause, le CEPD recommande à la Commission d'envisager la possibilité de les séparer des dispositions relatives aux communications électroniques qui ne sont pas liées à la vie privée ou à la protection des données.

Étant donné que le fondement juridique spécifique peut exiger l'adoption d'un nouvel instrument juridique, l'instrument comprenant les nouvelles dispositions en matière de vie privée et de communications électroniques devrait faire référence au RGPD et s'aligner sur celui-ci, en particulier pour ce qui est de ses définitions, de son champ d'application concernant les personnes morales, des données autres que celles à caractère personnel (métadonnées, sécurité, etc.) et de l'ensemble des éléments à l'appui de la mise en œuvre.

Quoi qu'il en soit, le CEPD recommande au législateur de se concentrer davantage sur les dispositions qui s'avèrent nécessaires, pour ensuite tirer parti des dispositions du RGPD en permettant aux autorités chargées de la protection des données (APD) d'émettre des orientations pour traiter avec souplesse l'évolution des nouvelles technologies, au travers des mécanismes mis à la disposition du comité européen de la protection des données par le RGPD, par exemple en matière de codes de conduite et de certifications.

III.4 Relation avec le cadre pour les communications électroniques

Dans les documents de sa consultation publique, la Commission ne prend pas clairement position sur la relation future entre un instrument en matière de vie privée et de communications électroniques, adopté dans le cadre du programme REFIT, et le cadre législatif relatif aux communications électroniques. Actuellement, la directive «vie privée et communications électroniques» est l'une des directives particulières visées dans la directive-cadre[13]. Cela signifie que, par exemple, les définitions de la directive-cadre sont utilisées dans la directive «vie privée et communications électroniques» et qu'elles doivent être interprétées de manière cohérente pour tous les aspects couverts par le cadre, c'est-à-dire aussi bien pour la vie privée que pour la gestion du spectre radioélectrique et la réglementation économique.

La décision de la Commission d'engager des procédures concernant la directive «vie privée et communications électroniques», apparemment sans les inclure dans un réexamen du cadre global, indique que les dispositions futures en matière de vie privée et de communications électroniques ne devraient plus faire partie intégrante du cadre législatif relatif aux communications électroniques. Le CEPD serait favorable à une telle approche, qui pourrait contribuer à surmonter les difficultés posées par la législation actuelle. En particulier, dans un tel scénario, le champ d'application et les définitions pourraient être arrêtés en fonction des objectifs spécifiques des futures dispositions en matière de vie privée et de communications électroniques, sans qu'il faille les concilier avec les nécessités de la réglementation économique. En outre, il serait plus facile de remédier au chevauchement potentiel de responsabilités entre les autorités de contrôle chargées de la protection des données et les autres autorités responsables du contrôle et de l'application des règles en matière de communications électroniques (voir aussi la section VII ci-dessous sur le *contrôle et l'application des règles*).

IV. CHAMP D'APPLICATION DU NOUVEL INSTRUMENT JURIDIQUE EN MATIÈRE DE VIE PRIVÉE ET DE COMMUNICATIONS ÉLECTRONIQUES

Historiquement, les droits à la confidentialité des communications trouvent leur origine dans le droit à la confidentialité des messages envoyés ou reçus par la poste. Afin de prendre en considération les évolutions technologiques, ce droit constitutionnel s'est étendu au fil du temps à d'autres moyens de communication, tels que le télégraphe et la téléphonie traditionnelle. Compte tenu des nouvelles évolutions technologiques, notamment l'apparition de communications passant par des fournisseurs de services dits «par contournement»[14], il est temps de procéder à une nouvelle extension de la protection.

Il est nécessaire d'actualiser les règles afin qu'elles couvrent les nouveaux types de prestation de 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.

La difficulté consiste à faire en sorte que toute nouvelle disposition reste suffisamment neutre sur le plan technologique afin de couvrir de nouveaux services, tout en offrant la sécurité juridique et la prédictibilité nécessaires. Par ailleurs, le champ d'application doit être étendu de telle manière qu'il assure un niveau élevé de protection pour les utilisateurs et, dans le même temps, des conditions de concurrence plus équitables des organisations concernées.

Enfin, les nouvelles dispositions en matière de vie privée et de communications électroniques doivent indiquer clairement et sans ambigüité les organisations visées et les exigences particulières auxquelles celles-ci doivent se conformer. Les définitions devront dès lors être repensées. Les définitions utilisées dans la directive «vie privée et communications électroniques» actuelle ont été conçues à des fins générales de réglementation économique dans le secteur des télécommunications et ne visent pas spécifiquement à protéger la vie privée. Le sens des termes «réseaux publics de communications électroniques» et «services de communications électroniques» n'est pas assez clair et ne reflète pas les réalités technologiques actuelles. Ces définitions ne tiennent pas compte des tendances à la convergence: l'estompement des rôles des fournisseurs de réseaux, des opérateurs de réseaux virtuels et des fournisseurs de services de communications par contournement, tels que les fournisseurs de services de messagerie vocale et écrite sur l'internet. Elles restent une source d'incertitude aussi bien pour les régulateurs que pour les organisations commerciales[15].

IV.1 Messagerie instantanée et voix sur IP

Du point de vue de l'utilisateur, les moyens de communication tels que la ligne de téléphone fixe traditionnelle ou les services de messagerie et de téléphonie mobile (SMS, MMS), d'une part, et les services de communications par contournement tels que la voix sur IP (VoIP[16]) et les applications de messagerie instantanée, d'autre part, sont équivalents sur le plan fonctionnel. Les personnes physiques doivent se voir accorder le même niveau de protection pour l'ensemble des services équivalents sur le plan fonctionnel, qu'ils soient fournis par des compagnies de téléphone traditionnelles, des services de voix sur IP ou des applications de messagerie sur téléphone mobile.

Au vu de ce qui précède, le champ d'application de la directive «vie privée et communications électroniques» pourrait être étendu pour couvrir au moins ces services, qui visent à fournir des services équivalents sur le plan fonctionnel aux services traditionnels de communications électroniques pour la communication audio, vidéo et écrite (par exemple, fournisseurs de voix

sur IP et de messagerie instantanée tels que Skype, Viber, FaceTime, WhatsApp, Signal, Threema, iMessage ou Facebook Messenger).

Toutefois, pour que les nouvelles dispositions en matière de vie privée et de communications électroniques puissent résister réellement à l'épreuve du temps et offrir un cadre neutre sur le plan technologique, assorti d'un niveau élevé de protection, il est nécessaire d'aller plus loin, en protégeant non seulement les communications « équivalentes sur le plan fonctionnel» à celles offertes par les fournisseurs traditionnels de services de télécommunications, mais aussi les services qui offrent de nouvelles possibilités de communication, éventuellement en complément d'autres offres.

Le CEPD recommande également à la Commission d'évaluer la nécessité et la possibilité de couvrir une gamme encore plus large de services. Par exemple, il conviendrait d'apprécier attentivement si les fonctions de communication intégrées à d'autres services (par exemple, les fonctions de messagerie dans les jeux vidéo ou les applications de rencontre) devraient également bénéficier d'une protection identique ou similaire. L'argument en faveur d'une extension de la protection se fonde sur le fait que les attentes de l'utilisateur sont souvent les mêmes en ce qui concerne le respect de la vie privée et de la confidentialité de ces messages et que toute violation de la confidentialité peut être tout autant attentatoire à la vie privée. 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 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.

IV.2 L'internet des objets

La directive «vie privée et communications électroniques» s'applique aux services «*sur les réseaux de communication [...] y compris les réseaux de communications publics qui prennent en charge les dispositifs de collecte de données et d'identification*» (article 3). Cette disposition précise que la finalité et le contenu d'une communication ne peuvent affecter la protection dont celle-ci jouit au titre du droit à la vie privée. Elle garantit que la protection de la confidentialité des communications ne dépend pas du fait que les personnes parlent ou écoutent ou qu'elles écrivent ou lisent le contenu d'une communication mais du fait qu'elles peuvent se fier aux caractéristiques de plus en plus intelligentes de leurs terminaux pour communiquer du contenu en leur nom, en bénéficiant du niveau de protection attendu. 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.

En réalité, ce que nous appelons l'«internet des objets» est essentiellement un «internet des objets connectés aux personnes». L'internet des objets (IdO) comprend les traceurs sportifs, les capteurs de santé, les appareils de communications personnelles, les téléviseurs intelligents observant leurs utilisateurs, les voitures intelligentes détectant tout mouvement de leurs passagers et bien d'autres appareils encore. Ils sont équipés de capteurs détectant le son, l'image, le mouvement et les paramètres physiques de leur propriétaire. Le fait qu'ils déclenchent 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.

Du point de vue d'un fournisseur de communications soumis à l'instrument en matière de vie privée et de 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.

Le CEPD recommande que les nouvelles dispositions en matière de vie privée et de communications électroniques continuent à s'appliquer sans ambiguïté aux communications de machine à machine dans le contexte de l'internet des objets, quel que soit le type de réseau ou de service de communications utilisé. La confidentialité et la sécurité de toute communication électronique à partir d'un appareil IdO (équipement terminal) et vers celui-ci devraient être couvertes, sur tous les réseaux et pour tous les services visés. Cela s'applique à toutes les dispositions pertinentes, en particulier les obligations de confidentialité énoncées à l'article 5, mais aussi les articles 6 et 9 concernant les données relatives au trafic et les données de localisation.

IV.3 Couverture de différents types de réseaux

La directive «vie privée et communications électroniques» détermine son champ d'application en utilisant des définitions tirées de la directive-cadre[17]. Ces définitions ont été conçues de sorte à couvrir une multitude de finalités, y compris la réglementation du marché, la gestion du spectre, l'accès universel, etc. Dans ce domaine complexe, les définitions générales ne peuvent recouvrir que l'intersection de tous les champs d'application et ne sont pas adaptées aux besoins spécifiques de la protection de la vie privée. En outre, la terminologie utilisée dans ces définitions a souvent été mal comprise. Par exemple, certains auteurs interprètent encore à tort le terme «réseaux publics» comme désignant les «réseaux appartenant au secteur public», tel qu'il est parfois utilisé dans d'autres contextes.

Pour des dispositions autonomes en matière de vie privée et de communications électroniques, il n'est plus nécessaire de faire en sorte que leur champ d'application soit équivalent à celui d'un instrument permettant la réglementation du marché. Le CEPD recommande que les nouvelles dispositions en matière de vie privée et de communications électroniques garantissent aussi –en principe – que les utilisateurs bénéficient de la même protection sur tous les réseaux auxquels ils peuvent accéder. Il recommande une extension qui ferait tomber sous le coup des exigences de confidentialité au moins tous les réseaux et services accessibles au public (y compris ceux fournis dans un but non lucratif). Seraient par exemple couverts 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 leurs hôtes et les endroits névralgiques créés par les administrations publiques.

Le CEPD recommande par ailleurs que le nouvel instrument juridique en matière de vie privée et de communications électroniques précise aussi ce qu'il convient d'entendre par «accessibles au public». Par exemple, il conviendrait de clarifier qu'un service reste 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 ses visiteurs.

Ces observations s'inscrivent dans le droit fil de celles formulées précédemment par le CEPD à ce sujet. 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[18], 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[19], 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).

V. PROTECTION DE LA CONFIDENTIALITÉ DES COMMUNICATIONS

La protection de la confidentialité des communications (article 5) doit rester un objectif clé du nouvel instrument juridique en matière de vie privée et de communications électroniques. Le CEPD réitère l'importance centrale du droit à la confidentialité des communications consacré par l'article 7 de la charte. Par ailleurs, il insiste sur l'importance de protéger aussi bien les communications en transit que les communications entreposées. Il souligne également que les nouveaux paradigmes techniques (par exemple, l'informatique en nuage) renforcent encore plus l'importance de la confidentialité[20].

Le CEPD attire également l'attention sur le fait qu'il n'existe pas de distinction claire entre le contenu et les «données relatives au trafic» dans un environnement multiservices tels 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 données relatives au trafic pour un autre[21].

Le traitement de données concernant la communication (comme les adresses URL des sites web consultés, l'intitulé du courriel, les données relatives au trafic et les données de localisation) est souvent tout aussi révélateur, voire davantage encore, que le contenu même de la communication.

De nombreux exemples en attestent. Par exemple, les métadonnées permettent l'identification de cibles lors d'opérations militaires à l'aide de drones[22]. Les métadonnées peuvent également servir à identifier des structures dans le cadre d'attentats politiques et d'enquêtes pénales[23]. 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[24]. 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, ses pratiques religieuses et même ses infidélités conjugales, peuvent être découverts à partir des données relatives au trafic tirées de son téléphone mobile[25].

Le nouvel instrument juridique en matière de vie privée et de communications électroniques doit dès lors prévoir clairement la protection de la confidentialité des communications, aussi bien du «contenu» que des «métadonnées» (y compris les données relatives au trafic et les données de localisation).

V.1 Article 5, paragraphe 1: protection des communications en transit

Le CEPD recommande que le nouvel instrument juridique en matière de vie privée et de communications électroniques maintienne l'interdiction générale de l'interception et de la surveillance des communications, en couvrant clairement et spécifiquement le contenu et les «métadonnées» (y compris les données relatives au trafic). Il recommande également d'étendre le champ d'application de cette interdiction comme indiqué ci-dessus.

Par ailleurs, afin de garantir la sécurité juridique, le CEPD recommande que les nouvelles dispositions en matière de vie privée et de communications électroniques clarifient les définitions actuelles des termes «communication», «données relatives au trafic» et «données de localisation». Ces éclaircissements devraient être intégrés dans le corps même de l'instrument juridique en matière de vie privée et de communications électroniques et complétés par une liste d'exemples pour chaque définition dans les considérants. Les dispositions devraient par exemple préciser si une adresse URL complète (indiquant la page web visitée) est considérée comme constituant des données relatives au contenu ou au trafic. Elles devraient également préciser de manière plus claire que la notion de communication n'inclut pas seulement les communications électroniques entre deux personnes physiques, mais aussi toute communication au sein d'un groupe défini (par exemple, une audioconférence ou des messages envoyés à un groupe défini de destinataires).

Le CEPD recommande également que les dispositions futures précisent que les notions d'interception et de surveillance doivent être interprétées au sens technologique le plus large qui soit, et qu'elles incluent l'ajout d'identifiants uniques dans la communication, par exemple des identifiants publicitaires, des balises audio ou des témoins de connexion permanents.

V.2 Article 5, paragraphe 3: protection de l'équipement terminal

Le CEPD recommande de maintenir et de renforcer l'exigence de consentement prévue actuellement à l'article 5, paragraphe 3. Il rappelle également que le consentement visé à l'article 5, paragraphe 3, devra être défini et interprété de la même manière que dans le RGPD.

L'article 5, paragraphe 3, protège l'intégrité des appareils des utilisateurs contre toute forme de manipulation non autorisée ou d'attaque. C'est l'une des règles de cybersécurité les plus spécifiques de la législation de l'Union européenne. Lorsque le terminal de l'utilisateur n'est pas protégé contre des interférences, le contenu des communications est, pour sa part, uniquement protégé sur le réseau, mais peut être intercepté, altéré ou détruit par une interaction malveillante avec le terminal de l'utilisateur avant d'être envoyé ou après être arrivé à destination: les transmissions de texte ou de données peuvent être lues ou modifiées sur le téléphone mobile; les mots de passe et les numéros d'identification personnels (codes PIN), dérobés sur des appareils de l'utilisateur; et les caméras et microphones incorporés, transformés en outils d'espionnage. L'article 5, paragraphe 3, prévoit une protection juridique contre ce genre de manipulation et d'abus. Un niveau de protection au moins équivalent sera nécessaire à l'avenir, étant donné que les appareils des utilisateurs renferment de plus en plus de données importantes et d'identifiants critiques. À cet égard, le CEPD rappelle son avis nº 8/2015 du 15 décembre 2015 sur la diffusion et l'utilisation de technologies de surveillance intrusive dans

lequel il a fait observer que «*la protection efficace des systèmes informatiques contre toute attaque ou toute interception illicite est essentielle pour protéger les droits fondamentaux au respect de la vie privée et à la protection des données des personnes physiques au sein de l'UE*».

Dans le même temps, les utilisateurs devraient pouvoir exercer un contrôle réel sur l'utilisation de témoins de connexion et d'outils similaires. Cela implique notamment la possibilité de choisir l'appareil et ses caractéristiques, ses améliorations ultérieures par l'ajout de composants et de logiciels et la configuration de toute caractéristique concernant le fonctionnement de l'appareil. Le considérant 66 de la directive 2009/136/CE[26] (directive sur les droits des utilisateurs) reconnaît déjà le droit de l'utilisateur de contrôler, à travers les caractéristiques techniques, le comportement de son appareil à l'égard de sa vie privée. Dans un environnement où la prolifération des attaques et des abus prend les proportions d'un secteur d'activité, il est inacceptable de restreindre le droit des utilisateurs de choisir les caractéristiques techniques qui protègent leurs appareils contre les interférences de tiers. Ce droit doit aussi comprendre le droit de choisir les éléments de contenu tiers qui sont exécutés et d'en bloquer d'autres, par exemple les scripts qui déclenchent des interactions entre l'appareil de l'utilisateur et des services d'échange d'annonces ou d'autres serveurs similaires.

Le consentement doit être libre

Si le CEPD recommande de maintenir l'exigence de consentement actuelle, il reconnaît aussi que l'article 5, paragraphe 3, tel qu'il est appliqué actuellement, n'a pas pleinement concrétisé son potentiel d'offrir une véritable possibilité de choix et de rendre 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 ce qu'il advient de leurs données.
Ce phénomène est parfois désigné sous le terme d'«accès subordonné à l'acceptation de témoins de connexion» ou «cookie-walls». Les accès subordonnés à l'acceptation de témoins de connexion ont pour effet d'empêcher les utilisateurs qui n'acceptent pas les témoins de connexion d'accéder aux sites web qu'ils veulent consulter[27]. Bon nombre de ces témoins de connexion suivent 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 accès subordonnés à l'acceptation de témoins de connexion 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. Non seulement le RGPD, qui représente une amélioration par rapport à la directive 95/46/CE, exige clairement que le consentement soit libre, mais il fournit désormais aussi de nouvelles orientations quant à ce que l'on entend par consentement libre. Il prévoit, entre autres, 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[28]. Tel est précisément le cas des accès subordonnés à l'acceptation de témoins de connexion, qui obligent souvent l'utilisateur à

consentir à l'utilisation de témoins de connexion de traçage de tiers qui ne sont pas nécessaires à la prestation du service concerné.

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 aux législateurs d'envisager une interdiction totale ou du moins partielle desdits «accès subordonnés à l'acceptation de témoins de connexion».

En cas d'interdiction complète de ces accès subordonnés à l'acceptation de témoins de connexion, les nouvelles dispositions en matière de vie privée et de communications électroniques devraient prévoir 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 5, paragraphe 3. Cette approche garantirait le niveau de protection le plus élevé pour les personnes physiques, ainsi que la sécurité juridique et des conditions de concurrence équitables à l'ensemble des acteurs du marché.

Subsidiairement, en cas d'interdiction partielle, les législateurs pourraient s'attacher tout spécialement aux situations les plus extrêmes, lorsque les répercussions sur les utilisateurs sont les plus fortes, ou lorsque leur liberté de choix est la plus faible. Dans ce cas, le nouvel instrument juridique en matière de vie privée et de communications électroniques pourrait prévoir une liste non exhaustive de situations dans lesquelles le choix n'est pas considéré comme ayant été effectué librement. Dans le même temps, il pourrait autoriser le comité européen de la protection des données à formuler de nouvelles orientations et à préciser les situations supplémentaires dans lesquelles les accès subordonnés à l'acceptation de témoins de connexion sont interdits. L'intérêt de cette approche réside dans sa souplesse, mais elle est susceptible de fournir un niveau plus faible de protection pour les personnes physiques, une sécurité juridique moindre et des conditions de concurrence moins équitables.

En cas d'interdiction partielle, le CEPD recommande d'inclure au moins les situations suivantes dans la liste non exhaustive arrêtée dans les nouvelles dispositions en matière de vie privée et de communications électroniques:

- les situations dans lesquelles le fournisseur du service se trouve dans une position dominante pour les services recherchés par l'utilisateur;
- toute autre situation dans laquelle il existe un rapport de force déséquilibré entre l'utilisateur et le fournisseur de services (les détails devront être précisés au besoin par le comité européen de la protection des données);
- les communications et les services financés totalement ou partiellement par l'argent du contribuable (par exemple, les sites web proposant des services administratifs en ligne, les organes de presse soutenus par des subventions publiques ou des redevances obligatoires);
- toute situation dans laquelle des catégories spéciales de données peuvent être déduites des données collectées, prises soit en l'état soit en combinaison avec d'autres données (par exemple, consultation de sites d'actualité, de sites d'information sur la santé ou de librairies en ligne, utilisation d'applications de mise en forme, traçage de données de localisation dans un lieu de culte ou un hôpital);

- les situations dans lesquelles un site web ou une application vend aux enchères ses espaces publicitaires et dans lesquelles des tiers peuvent suivre à la trace et surveiller les utilisateurs à travers le site web ou l'application;
- le consentement groupé à des fins multiples (par exemple, lorsque le consentement pour la commercialisation et pour les services à valeur ajoutée ne peut être donné ou retiré séparément).

Si l'interdiction n'est que partielle, le CEPD recommande que les nouvelles dispositions en matière de vie privée et de communications électroniques prévoient en outre que, quelle que soit la puissance commerciale du fournisseur de services, celui-ci doit i) soit offrir le choix de consentir au traitement de données qui ne sont pas nécessaires à la prestation du service sans nuire à l'utilisateur, ii) soit au moins proposer un service payant à un prix raisonnable (sans publicité comportementale ni collecte de données) à la place des services payés par les informations à caractère personnel des utilisateurs. Cette possibilité a déjà été évoquée par la Commission dans sa consultation publique[29].

Mécanismes d'octroi et de retrait du consentement

Enfin, le CEPD souligne que les utilisateurs doivent disposer de mécanismes efficaces et faciles à utiliser pour donner et retirer leur consentement. S'appuyant sur le considérant 66 susmentionné de la directive sur les droits des utilisateurs, le CEPD recommande que les nouvelles dispositions en matière de vie privée et de communications électroniques prévoient une exigence légale réaliste garantissant que le consentement de l'utilisateur au traitement peut être exprimé en utilisant les paramètres appropriés d'un navigateur ou d'une autre application.

Cela signifie qu'au lieu de s'en remettre purement et simplement aux exploitants de sites web pour obtenir le consentement au nom de tiers (comme les réseaux publicitaires et les réseaux sociaux), le nouvel instrument juridique en matière de vie privée et de communications électroniques pourrait exiger que les navigateurs et les autres logiciels ou systèmes d'exploitation intègrent des outils de contrôle tels que l'interdiction du suivi («Do Not Track», DNT) ou d'autres moyens techniques permettant aux utilisateurs d'exprimer aisément leur consentement ou leur non-consentement.

Ces outils doivent être proposés à l'utilisateur lors de la configuration initiale au moyen d'un paramétrage par défaut respectueux de la vie privée.

L'ensemble des 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.

Nécessité d'une formulation plus vaste et neutre sur le plan technologique

Par ailleurs, la formulation actuelle de l'article 5, paragraphe 3 – «*le stockage d'informations*» ou «*l'obtention de l'accès à des informations déjà stockées*» dans l'équipement terminal d'utilisateurs – a laissé une certaine marge pour l'apparition d'interprétations divergentes quant à la question de savoir quels types d'interaction entre un tiers et l'appareil d'un utilisateur sont couverts, notamment en ce qui concerne l'«*obtention de l'accès à des informations déjà stockées*». S'il est manifeste que toute interférence non autorisée avec l'appareil devrait être couverte, il existe des cas moins évidents. La collecte et l'utilisation des informations que

l'appareil de l'utilisateur fournit par défaut dans le cadre d'un comportement standard en matière de communications peuvent-elles être considérées comme l'obtention de l'accès à des informations déjà stockées? Si les informations ne sont pas fournies par défaut, une demande d'informations prise en charge par le protocole de communication utilisé entre le terminal et le tiers peut-elle être considérée comme une obtention de l'accès? Les informations qui sont uniquement produites en réponse à une demande d'un tiers (par exemple, le niveau de la batterie mesuré en réponse à la demande) devraient-elles être considérées comme des informations déjà stockées? Comment considérer les informations associées au terminal de l'utilisateur et accessibles par son intermédiaire, sans y être stockées physiquement, et téléchargées à partir d'un service en nuage pour répondre à la demande du tiers?

Le CEPD considère que, à la lumière des exemples cités ci-dessus, la mise en œuvre technique ne devrait pas servir de critère pour déterminer le niveau de protection de la vie privée de l'utilisateur, d'autant plus que, dans certains cas, il est possible que ni l'utilisateur, ni le tiers qui demande les informations n'aient pas connaissance des circonstances techniques exactes d'une demande d'informations. Par conséquent, la formulation de l'instrument devrait être la plus inclusive et la plus neutre possible sur le plan technologique. Il convient, par exemple, 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.

Exception applicable aux témoins analytiques d'origine

Par ailleurs, tout en précisant le champ d'application de l'exigence de consentement, le nouvel instrument juridique en matière de vie privée et de communications électroniques devrait également prévoir une exception pour les témoins analytiques d'origine, sous réserve des garanties adéquates[30]. 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 recommande 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[31], le groupe de travail «Article 29» sur la protection des données a déjà appelé les législateurs à établir une telle exception.

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 nouvel instrument juridique en matière de vie privée et de communications électroniques pourrait faire référence aux orientations futures qui seront fournies par le comité européen de la protection des données.

V.3 Données relatives au trafic et données de localisation

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.

Ces données ne sont plus collectées uniquement par les compagnies de téléphone traditionnelles et les fournisseurs d'accès à l'internet. Toute une série de nouveaux fournisseurs de services peuvent également obtenir un aperçu très détaillé des habitudes de voyage et de communication d'un utilisateur, de ses réseaux sociaux, etc. Dans le même temps, ces fournisseurs de services ne sont pas soumis, à l'heure actuelle, aux obligations de la directive «vie privée et communications électroniques».

En exigeant le consentement pour le traitement des données relatives au trafic et des données de localisation, la directive «vie privée et communications électroniques» actuelle offre un niveau de protection plus élevé que le RGPD. Celui-ci prévoit, au moins potentiellement, d'autres fondements juridiques, tels que les intérêts légitimes ou l'exécution d'un contrat. Un responsable du traitement pourrait tenter de faire valoir, par exemple, que le traçage des utilisateurs sur l'internet et la constitution de profils détaillés qui leur correspondent font partie de son intérêt légitime à commercialiser ses services et produits.

Afin de mieux protéger la confidentialité des communications électroniques, le CEPD recommande que la directive «vie privée et communications électroniques» maintienne et renforce l'exigence de consentement actuelle pour les données relatives au trafic et les données de localisation. Il recommande en particulier de réviser ladite directive pour y inclure une exigence de consentement unique pour le traitement des métadonnées. Cela devrait s'appliquer à l'ensemble des données relatives au trafic et des données de localisation, quelle que soit la personne qui collecte et traite ces données. Autrement dit, la portée de cette disposition devrait, comme dans le cas de l'article 5, paragraphe 3, être élargie afin de couvrir toute personne et pas uniquement les compagnies de téléphone traditionnelles et les fournisseurs d'accès à l'internet.

VI. PROTECTION DE LA SÉCURITÉ DES COMMUNICATIONS

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 qui existent dans la directive «vie privée et communications électroniques».

Les exigences de sécurité du RGPD ne s'appliquent qu'aux cas concernant des données à caractère personnel. Il est cependant nécessaire de faire en sorte que d'autres données, par exemple les informations commerciales confidentielles, qui ne contiennent pas nécessairement de données à caractère personnel, restent protégées. D'autres instruments juridiques, tels que la directive relative à la cybersécurité[32], ne couvrent eux aussi que certaines situations.

Par conséquent, des dispositions particulières sur la sécurité restent également nécessaires dans le nouveau cadre juridique en matière de vie privée et de communications électroniques[33].

Par ailleurs, il ne devrait y avoir aucune ambigüité quant au champ d'application de toute exigence visant à protéger la sécurité des communications: les nouvelles dispositions en matière de vie privée et de communications électroniques devraient prévoir clairement (dans le corps même du texte, et pas seulement dans un considérant) la confidentialité et la sécurité des communications en transit, mais également protéger la confidentialité et la sécurité de

l'équipement de l'utilisateur final. Le CEPD recommande de revoir l'article 4 de la directive «vie privée et communications électroniques» de manière à couvrir clairement ces deux situations. Les nouvelles dispositions en matière de vie privée et de communications électroniques devraient également garantir que l'article 5, paragraphe 3 – ou une disposition similaire – continue à protéger l'équipement de l'utilisateur final contre les logiciels espions.

VI.1 Nécessité de mesures supplémentaires sur la sécurité dans les nouvelles dispositions en matière de vie privée et de communications électroniques

Le CEPD considère également que les mesures supplémentaires suivantes sur la sécurité, mentionnées dans la consultation publique de la Commission[34], seraient nécessaires:

- 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.

Les normes peuvent étendre les exigences de sécurité de manière à assurer la couverture des fournisseurs de services de réseau, des fournisseurs de composants de réseau, des équipements terminaux (y compris l'IdO) ou complémentaires (y compris les logiciels) utilisés en combinaison avec la fourniture de services de communications électroniques.

VI.2 Chiffrement

Comme le GT29 l'a également relevé, *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*[35].

Le CEPD recommande que les nouvelles dispositions en matière de vie privée et de comunications électroniques autorisent clairement les utilisateurs à recourir au chiffrement de bout en bout (sans «porte dérobée»[36]) pour protéger leurs communications électroniques. Par ailleurs, le CEPD recommande, comme le suggère aussi le GT29, 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 nouvel instrument juridique en matière de vie privée et de 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».

VI.3 Violations de données

Le CEPD recommande la suppression de l'article 4, paragraphes 3 et 4, de la directive «vie privée et communications électroniques» relatifs aux violations de données, étant donné que le RGPD impose déjà à tous les responsables du traitement de notifier les violations de données à caractère personnel aux abonnés et aux autorités nationales compétentes (sous réserve de certaines exemptions). Pour éviter les doublons, nous recommandons que toutes les violations portant sur des données à caractère personnel soient communiquées aux autorités de contrôle prévues dans le RGPD, conformément aux dispositions de ce dernier.

VII. SURVEILLANCE ET CONTRÔLE DE L'APPLICATION

En vertu de la directive «vie privée et communications électroniques» actuelle, plusieurs autorités différentes sont responsables de la surveillance et du contrôle de l'application des différentes dispositions de la directive. L'expérience révèle des différences significatives au sein de l'Europe, mais aussi des chevauchements ou des doublons entre les rôles des diverses autorités de contrôle[37]. Il est par conséquent nécessaire de simplifier le cadre existant.

Il convient en outre de garder à l'esprit que le RGPD impose de nouvelles obligations aux autorités de contrôle, telles que la coopération entre les autorités nationales compétentes, le mécanisme de cohérence et le rôle du comité européen de la protection des données. Si le contrôle du nouvel instrument juridique en matière de vie privée et de communications électroniques (ou de certaines parties de celui-ci) devait être exécuté par une autorité qui n'est pas chargée de la protection des données, un mécanisme efficace devrait être conçu pour que cette autorité soit représentée au sein des mécanismes de coopération entre les autorités de protection des données. Cela pourrait rendre le dispositif de coopération encore plus complexe qu'il ne l'est aujourd'hui.

Au vu de ces considérations, dans tous les cas où une tâche peut être efficacement exécutée par une autorité nationale de protection des données, le CEPD recommande de la considérer comme l'autorité compétente dans un souci de sécurité juridique et pour faciliter la mise en œuvre pratique.

VIII. COMMUNICATIONS NON SOLLICITÉES

Le CEDP recommande de maintenir, d'actualiser et de renforcer les règles actuelles de la directive «vie privée et communications électroniques» offrant une protection contre les communications non sollicitées.Lors du réexamen, 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.

Le CEPD recommande par conséquent que les nouvelles dispositions en matière de vie privée et de communications électroniques adoptent une approche neutre sur le plan technologique. L'article 13 devrait exiger 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 – c'est-à-dire dans le cadre d'un service de la société de l'information – et publicité comportementale). Par ailleurs, le niveau de protection devrait être équivalent, que l'utilisateur/abonné soit une personne physique ou morale.

Les exceptions actuelles concernant les relations existantes et les produits et services similaires devraient être préservées, mais le CEPD recommande que les nouvelles dispositions en matière de vie privée et de communications électroniques précisent ce qu'il y a lieu d'entendre par «relation existante» et «produits et services similaires».

La directive «vie privée et communications électroniques» actuelle porte principalement sur les communications «commerciales». Or, toutes les communications non sollicitées ou malveillantes ne peuvent être considérées comme commerciales au sens habituel du terme. À proprement parler, les communications liées à des tentatives criminelles, par exemple les attaques par hameçonnage et les propositions financières frauduleuses, peuvent ne pas toujours être couvertes par cette qualification. Il est recommandé au législateur de vérifier s'il est possible de fournir une définition 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.

IX. ANNUAIRES D'ABONNÉS

L'article 12 de la directive «vie privée et communications électroniques» prévoit le droit des abonnés de «*décider si les données à caractère personnel les concernant [...]doivent figurer dans un annuaire public [imprimé ou électronique]*».

Le CEDPD recommande de maintenir cette disposition et d'élargir son champ d'application de manière à inclure tout type de services d'annuaires. Par ailleurs, 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.

X. RECOMMANDATIONS COMPLÉMENTAIRES

X.1 Identification de la ligne appelante (CLI)

La directive «vie privée et communications électroniques» 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 recommande de maintenir ce droit comme étant 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.

X.2 Champ d'application territorial et droit applicable

Le CEPD recommande que les nouvelles dispositions en matière de vie privée et de communications électroniques aient en principe, et sans ambiguïté, le même champ d'application que le RGPD (y compris le champ d'application extraterritorial visé à l'article 3, paragraphe 2[38]) et qu'elles suivent en principe la même approche en ce qui concerne le droit applicable au traitement des données à caractère personnel.

Dans le même temps, la nécessité éventuelle de procéder à certains ajustements techniques dans la formulation de ces dispositions doit être envisagée. Par exemple, l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» s'applique, que la personne qui met en place un témoin de connexion ou déploie un logiciel espion soit considérée ou non comme un «responsable du traitement» aux termes du RGPD, et que des données à caractère personnel soient traitées ou non. Par conséquent, il pourrait être nécessaire de refléter ces différences dans le champ d'application territorial.

X.3 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. D'un côté, les communications entre les États membres de l'Union européenne peuvent traverser des pays tiers; de l'autre, 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 seront fondées uniquement sur un accord international tel qu'un traité d'entraide judiciaire[39].

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.

Par conséquent, le CEPD recommande que les nouvelles dispositions en matière de vie privée et de communications électroniques comportent des règles particulières renforçant la transparence. Il recommande 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. 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.

XI. CONCLUSIONS

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,

(**signature**)

Giovanni BUTTARELLI

Contrôleur européen de la protection des données

Notes

[1] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive «vie privée et communications électroniques»), JO L 201 du 31.7.2002, p. 37, modifiée par la directive 2009/136/CE.

[2] Réf. Ares(2016)2310042 – 18.5.2016.

[3] Voir https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-eprivacy-directive. Le questionnaire est disponible à l'adresse suivante: https://ec.europa.eu/eusurvey/runner/EPRIVACYReview2016.

[4] Avis 3/2016 du GT29 sur l'évaluation et le réexamen de la directive «vie privée et communications électroniques» (2002/58/CE) (GT240) adopté le 19 juillet 2016.

[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 4.5.2016, 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 la note de fin de document 4.

[9] Voir https://edri.org/files/epd-revision/EDRi_ePrivacyDir-final.pdf.

[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] 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.

[13] 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.

[14] Le terme «par contournement» s'applique aux services et applications accessibles sur l'internet qui utilisent un réseau fourni pour offrir des services d'accès à l'internet. Parmi les exemples disponibles figurent les services de communications (vocales et écrites) tels que Skype, WhatsApp et Facebook Messenger, mais aussi une vaste gamme d'autres services et applications, tels que les réseaux sociaux comme Facebook, Twitter ou LinkedIn, et les services de diffusion audio et vidéo en continu tels que Netflix ou YouTube. Pour de plus amples informations sur le sujet, voir par exemple l'étude suivante: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/569979/IPOL_STU(2015)569979_EN.pdf.

[15] On remarquera également que souvent, un utilisateur peut engager une communication vocale ou écrite par l'intermédiaire d'un service de communications par contournement, alors que son destinataire peut recevoir le message ou participer à la communication par des moyens traditionnels (par exemple , il peut recevoir un SMS sur son téléphone mobile ou un appel VoIP sur sa ligne de téléphone fixe).

[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] Voir la note de fin de document 13.

[18] 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») (JO C 181 du 18.7.2008, p. 1), 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.

[19] 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») (JO C 128 du 6.6.2009, p. 28). 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.

[20] 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

[21] Pour des informations générales sur la technologie, voir les pages https://fr.wikipedia.org/wiki/Mod%C3%A8le_OSI concernant le modèle OSI et https://fr.wikipedia.org/wiki/Suite_des_protocoles_Internet concernant la suite des protocoles internet.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, 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 et le règlement (CE) nº 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs, JO L 337/2009 du 18.12.2009, p. 11, disponible à l'adresse suivante: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:fr:PDF.

[27] 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.

[28] Dans son 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*».

[29] Voir la question 22 de la consultation publique de la Commission: «Les fournisseurs de services de la société de l'information devraient être tenus de proposer un service payant (sans publicité comportementale) à la place des services payés par les informations à caractère personnel des utilisateurs».

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

[31] Avis 04/2012 du groupe de travail «Article 29» sur l'exemption de l'obligation de consentement pour certains cookies, disponible à l'adresse suivante: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_fr.pdf.

[32] 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.

[33] Cela étant, le RGPD et le nouvel instrument juridique en matière de vie privée et de 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).

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

[35] Voir l'avis du GT29 cité à la note de fin de document 4, p. 19.

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

[37] Étude intitulée «ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation» (SMART 2013/0071), section 3.2.3, *Supervision* (pp. 33 et 34), disponible à l'adresse suivante: https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data.

[38] Voir aussi l'analyse conjointe de certains groupes de la société civile visée à la note de fin de document 9 ci-dessus.

[39] Voir l'article 48 du RGPD «*Transferts de divulgations non autorisées par le droit de l'Union*».