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

16/FR

WP 240

Avis 03/2016 sur l'évaluation et la révision de la directive «vie privée et communications électroniques» (2002/58/CE)

Adopté le 19 juillet 2016

Ce groupe de travail a été institué par l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.

Le secrétariat est assuré par la direction C (Droits fondamentaux et état de droit) de la direction générale de la justice et des consommateurs de la Commission européenne, B-1049 Bruxelles, Belgique, bureau MO-59 02/013.

Site internet: http://ec.europa.eu/justice/data-protection/index_fr.htm

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

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

vu les articles 29 et 30 de ladite directive,

vu son règlement intérieur,

A ADOPTÉ LE PRÉSENT AVIS:

RÉSUMÉ

1. INTRODUCTION

Le développement du marché numérique, ainsi que la récente adoption du règlement (UE) 2016/679 (ci-après le «règlement général sur la protection des données» ou «RGPD») appellent à une révision en profondeur des règles de la directive 2002/58/CE (ci-après la «directive "vie privée et communications électroniques"»). La révision de cette directive doit déboucher sur un système réglementaire cohérent et efficace qui assure une plus grande sécurité juridique concernant les dispositions légales applicables à toute situation donnée. Depuis 2002, la directive «vie privée et communications électroniques» prévoit un certain nombre de mesures de protection de la sécurité et de la vie privée supplémentaires, principalement axées sur la téléphonie et les fournisseurs d'accès internet. Son article 1er, paragraphe 2, dispose que la directive a été adoptée afin de préciser et de compléter la directive 95/46/CE relative à la protection des données, qui sera abrogée par le RGPD lorsqu'il entrera en vigueur le 28 mai 2018[1].

Le groupe de travail «Article 29» (GT29) partage le point de vue de la Commission quant à la nécessité de disposer de règles spécifiques pour les communications électroniques au sein de l'UE. Si le RGPD est un développement juridique détaillé de l'article 8 de la charte des droits fondamentaux de l'Union européenne (ci-après la «Charte») relatif à la protection des données, l'article 7 de la Charte protège spécifiquement la confidentialité des communications. Ce droit de l'homme mérite également un développement juridique détaillé. Le nouvel instrument juridique doit compléter et étayer les obligations du RGPD afin de protéger spécifiquement la sécurité des communications électroniques.

Les règles du RGPD sont toujours applicables au traitement des données à caractère personnel, indépendamment de la nature des données ou du/des fournisseur(s) de services. Toutefois, conformément à son article 95, le RGPD ne peut pas imposer «*d'obligations supplémentaires aux personnes physiques ou morales quant au traitement dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communications dans l'Union en ce qui concerne les aspects pour lesquels elles sont soumises à des obligations spécifiques ayant le même objectif énoncées dans la directive 2002/58/CE*». Comme précisé au considérant 173, cette disposition vise à garantir que le RGPD ne s'applique pas dans les cas où la directive «vie privée et communications électroniques» contient des obligations spécifiques ayant le même objectif. Le RGPD s'applique cependant à tous les autres cas. L'actuelle directive «vie privée et communications électroniques» définit déjà un niveau de protection élevé en exigeant le consentement préalable des utilisateurs avant la collecte de contenus à partir de leurs données de communications, de leurs données relatives au trafic ou de leurs données de localisation, à l'exception d'un nombre limité de cas. Cette exigence de consentement limite donc les fondements juridiques pouvant être invoqués pour justifier la collecte de données à caractère personnel en vertu du RGPD. Afin d'assurer la cohérence avec l'article 95 du RGPD, le nouvel instrument «vie privée et communications électroniques» devrait au moins maintenir et renforcer ses principes actuels pour garantir la confidentialité des communications

[1] Journal officiel de l'Union européenne, L 119, vol. 59, du 4 mai 2016, URL: https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:L:2016:119:FULL

électroniques. Concernant le fondement juridique, et sans préjudice de l'application d'une obligation légale spécifique justifiant le traitement des données, il devrait être clair que l'exigence de consentement prévaut sur les autres fondements juridiques (tels que l'intérêt légitime du responsable du traitement) visés à l'article 6 du RGPD. Aussi, en vertu du nouvel instrument «vie privée et communications électroniques», les fournisseurs de services ne devraient-ils traiter des informations que lorsque ledit instrument – ou toute autre disposition législative qui s'y réfère expressément – le permet, ou lorsque le destinataire du service a donné son consentement préalable.

La nouvelle mesure législative «vie privée et communications électroniques» devrait également prévoir des règles supplémentaires afin de protéger la sécurité des communications électroniques. Cela comprend les données générées par des réseaux ou systèmes de communications électroniques qui ne sont pas ou ne sont plus des données à caractère personnel, ainsi que les données traitées par des parties qui ne peuvent pas être considérées comme des responsables du traitement ou des sous-traitants. Par conséquent, **le nouvel instrument fournirait une protection supplémentaire aux communications électroniques des personnes physiques et morales.**

En outre, dès lors que les données relatives au trafic, les données de communication et les données de localisation sont pour la plupart des données à caractère personnel, un certain chevauchement entre l'instrument «vie privée et communications électroniques» et le RGPD est inévitable. En pareil cas, la Commission européenne doit veiller à ce qu'outre un niveau élevé de confidentialité, le niveau de protection des données à caractère personnel du RGPD ne soit pas affaibli. **L'instrument «vie privée et communications électroniques» révisé devrait conserver la substance des dispositions existantes, mais aussi les rendre plus efficaces et applicables dans la pratique, en étendant le champ d'application des règles concernant les données de géolocalisation et les données relatives au trafic à toutes les parties, tout en introduisant des conditions plus détaillées qui tiennent pleinement compte du caractère intrusif du traitement des données de communication vis-à-vis de la vie privée des utilisateurs**.

Par ailleurs, le champ d'application de l'actuelle directive «vie privée et communications électroniques» est essentiellement limité aux services de communications électroniques traditionnels (tels que les fournisseurs de services internet et les entreprises de télécommunications). Nombre de ses dispositions ne s'appliquent par exemple pas à la téléphonie sur internet (VoIP) ou aux fournisseurs de services de messagerie électronique ou instantanée. Compte tenu de la grande dépendance de nombreux Européens vis-à-vis des communications électroniques, **le nouvel instrument juridique doit chercher à protéger la confidentialité des services de communications électroniques aux fonctionnalités équivalentes** (par exemple, WhatsApp, Google Gmail, Skype et Facebook Messenger), **notamment en ce qui concerne les messages échangés par et entre des individus et des groupes d'utilisateurs privés.**

Un autre problème de l'actuelle directive «vie privée et communications électroniques» réside dans les différences d'interprétation des définitions, et, partant, dans les différences entre les législations nationales et leur mise en œuvre. De telles différences de mise en œuvre sont également le résultat de la latitude laissée aux États membres concernant le caractère facultatif ou non de certaines restrictions de traitement (par exemple, article 12, paragraphe 3) et

l'application éventuelle d'obligations différentes pour les entreprises et les individus abonnés. La Commission européenne devrait avoir pour objectif de mettre en place un régime juridique cohérent à travers l'UE afin d'assurer une protection égale à tous les individus dans l'ensemble des États membres de l'UE, ainsi que des règles identiques pour tous les acteurs pertinents en Europe. **Dans la mesure où l'instrument «vie privée et communications électroniques» révisé est clair et univoque dans ses définitions et ses exigences, cet objectif pourrait être atteint au moyen d'une directive ou d'un règlement,** si un pouvoir discrétionnaire très limité est laissé aux États membres en ce qui concerne les activités législatives nationales relatives au niveau de protection.

2. CHAMP D'APPLICATION DE L'INSTRUMENT «VIE PRIVÉE ET COMMUNICATIONS ÉLECTRONIQUES»

EXTENSION DU CHAMP D'APPLICATION AUX NOUVEAUX FOURNISSEURS DE SERVICES PAR CONTOURNEMENT (SERVICES OTT)

Du point de vue de l'utilisateur, il existe une équivalence fonctionnelle entre les moyens de communication tels que la téléphonie fixe traditionnelle et les services internet, d'une part, et les services de téléphonie via internet et les applications de messagerie mobile, d'autre part. Dès lors que ces services utilisent des protocoles de voix sur IP (*Voice over IP protocols*), l'acronyme «VoIP», qui en principe se réfère à la technologie même, est souvent utilisé pour désigner ce type de services. Les protections juridiques de la directive «vie privée et communications électroniques» ne s'appliquent cependant en principe qu'aux fournisseurs de réseaux et services de communications accessibles au public car les règles correspondantes ont initialement été établies en partant du principe que seuls les services de transmission devraient être couverts par le cadre juridique et que les services de plus haut niveau dépassaient ce champ d'application[2].

En guise d'introduction aux questions abordées dans le chapitre 3, l'article 5, paragraphe 1, de l'actuelle directive «vie privée et communications électroniques» interdit l'interception de contenus et de données relatives au trafic y afférentes dans le réseau de base (fournisseurs de téléphonie et d'accès internet). En l'absence de règles strictes, les fournisseurs de services internet et les opérateurs de télécommunications seraient en mesure de suivre en temps réel les activités en ligne de tous leurs clients et de créer des profils détaillés, notamment parce qu'ils sont en mesure de traiter toutes les données de communication de leurs clients. **L'obligation de respecter la confidentialité des communications devrait également s'appliquer aux nouveaux acteurs sur le marché des communications proposant des fonctionnalités équivalentes[3], tels que les opérateurs de réseaux virtuels et les fournisseurs de services de communication qui constituent de proches substituts aux services correspondants proposés par les fournisseurs de télécommunications (par**

[2] Plus précisément, selon son article 3, la directive «vie privée et communications électroniques» s'applique «*au traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communications dans la Communauté*». Ces services devraient entièrement ou essentiellement consister en l'acheminement de signaux sur des réseaux de communications électroniques par opposition à la fourniture de contenu, par exemple.

[3] Les actuelles différences de régime juridique entraînent une inégalité de traitement entre les organisations, ainsi que des différences inacceptables dans la protection des droits fondamentaux des utilisateurs lorsque leurs données sont traitées dans le cadre de services très similaires (d'un point de vue fonctionnel) à des fins similaires.

exemple, voix sur IP non gérée, messagerie instantanée, messagerie web et messagerie sur les réseaux sociaux).

L'expression «services par contournement» (services over-the-top ou OTT) est souvent utilisée pour qualifier ces nouveaux services. Elle ne dispose toutefois pas de définition juridique claire et de références à des catégories existantes de services de communication. Dans son rapport sur les services OTT[4], l'ORECE définit les services OTT comme «du contenu, un service ou une application fournis à l'utilisateur final sur l'internet public» et divise ces services en trois catégories:

- les OTT-0 peuvent être qualifiés de services de communications électroniques (SCE);
- les OTT-1 sont des services qui ne tombent pas sous la définition actuelle des SCE, mais qui sont potentiellement en concurrence avec ceux-ci;
- les OTT-2 sont les autres services, c'est-à-dire tout (autre) service de la société de l'information.

La Commission européenne devrait proposer que le champ d'application de l'instrument «vie privée et communications électroniques» révisé comprenne tous les (ou une partie des) services qui permettent les communications individuelles et dans le cadre desquels les fournisseurs de services revêtent le rôle fonctionnel de vecteur de communications neutre. La Commission devrait détecter les éventuelles lacunes juridiques dans la situation actuelle qui représentent une menace pour le droit à la confidentialité des communications de façon générale. **La Commission européenne devrait proposer une définition claire des services aux fonctionnalités équivalentes devant respecter les exigences de confidentialité,** notamment lorsqu'ils correspondent à la définition des services OTT-1, qu'ils puissent ou non être également considérés comme des «services de la société de l'information»[5].

RÉVISION DES DÉFINITIONS

L'actuel cadre réglementaire européen[6] pour l'environnement en ligne distingue trois catégories de services: 1) les services de la société de l'information, 2) les services de communications électroniques et 3) les services de médias audiovisuels. Cette distinction s'est traduite par l'adoption respective de la directive sur le commerce électronique, de la réglementation en matière de communications électroniques et de la directive «services de médias audiovisuels».

À cet égard, le GT29 rappelle qu'il a observé dans son avis 02/2008 **que la définition des «réseaux publics de communications électroniques» et des «services de communications électroniques» est très souvent confuse et qu'elle ne reflète pas l'infrastructure des réseaux de communication d'aujourd'hui.** Ces définitions ne tiennent pas compte de l'effacement des frontières entre les rôles des fournisseurs de réseau, des opérateurs de réseau

[4] BEREC Report on OTT services, janvier 2016 - BoR (16) 35, URL: http://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/5751-berec-report-on-ott-services_0.pdf.

[5] Faute de quoi les services de la société de l'information ne relèveraient pas du champ d'application de l'instrument «vie privée et communications électroniques».

[6] Depuis la création de ce cadre réglementaire, le paysage des services de communication s'est transformé en une structure complexe composée de réseaux interconnectés et d'un large éventail d'entreprises de communication, dont certaines peuvent être établies à l'extérieur de l'UE.

virtuel et des fournisseurs de services de communication tels que les services OTT (par exemple, fournisseurs de téléphonie et de services de messagerie sur internet). Depuis l'avis adopté par le GT29 en 2008, cette question n'a pas reçu l'attention voulue de la part de la Commission européenne et reste une source d'incertitude pour les législateurs et les organisations concernées.

Dans ce contexte, les «services de la société de l'information» sont exclus du champ d'application de la plupart des dispositions de la directive «vie privée et communications électroniques»[7]. Si des services de communication aux fonctionnalités équivalentes sont qualifiés de «services de la société de l'information», il semblerait que leurs fournisseurs ne soient pas tenus de respecter les exigences de confidentialité définies par la directive «vie privée et télécommunications». Cette différence de traitement juridique des services aux fonctionnalités équivalentes constitue une menace au droit à la confidentialité des communications et nuit à l'instauration de règles identiques pour tous. La Commission européenne devrait donc identifier ces lacunes juridiques et évaluer et modifier les définitions.

Bien que certaines des règles de la directive «vie privée et communications électroniques» aient été étendues afin de s'appliquer à toutes les organisations pratiquant certaines activités – par exemple, marketing direct non sollicité (article 13) ou accès à des informations ou stockage d'informations sur l'appareil d'un utilisateur (article 5, paragraphe 3) –, ces extensions spécifiques ne compensent pas les lacunes manifestes dans la protection du secret des communications sur les réseaux et dans les communications électroniques modernes. Si le groupe de travail recommande globalement d'étendre le champ d'application général du nouvel instrument aux fournisseurs de services OTT-1, il estime également nécessaire d'étendre les règles spécifiques aux données de localisation et aux données relatives au trafic à toutes les organisations. La mise en place d'un champ d'application aussi vaste n'est pas une difficulté en soi, mais la Commission européenne doit veiller à ce que toute révision de l'instrument législatif assure une interprétation univoque quant à savoir quelles organisations doivent respecter quelles obligations spécifiques.

AJOUT DES RÉSEAUX DE COMMUNICATION «PRIVÉS ACCESSIBLES AU PUBLIC»

Le groupe de travail renvoie à l'avis de 2009[8] du CEPD relatif au réexamen de la directive «vie privée et communications électroniques», qui suggère d'inclure dans le champ d'application de la directive «*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 et* ***sur les réseaux privés accessibles au public*** *dans la Communauté*» (soulignement ajouté).

---

[7] 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), JO L 108 du 24.4.2002, p. 33, telle que modifiée par la directive 2009/140/CE et le règlement (UE) nº 544/2009. Conformément à l'article 2, point c), de la directive-cadre, la notion de «service de communications électroniques» ne comprend pas les services de la société de l'information, tels que définis à l'article 1er de la directive 98/34/CE. À cet égard, le considérant 5 de la directive-cadre dispose qu'il est nécessaire «*de séparer la réglementation de la transmission de celle des contenus*» et que le «*cadre ne s'applique donc pas aux contenus des services fournis sur les réseaux de communications électroniques à l'aide de services de communications électroniques, tels que les contenus radiodiffusés, les services financiers et certains services propres à la société de l'information*».

[8] 2e avis du CEPD relatif au réexamen de la directive «vie privée et communications électroniques», janvier 2009, par. 98, URL: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-01-09_ePricacy_2_FR.pdf

Un tel élargissement ferait entrer tous les réseaux et services accessibles au public (câblés ou sans fil, détenus ou gérés par un organisme public ou privé) dans le champ d'application des exigences de confidentialité (par exemple, les services WiFi dans les hôtels, les magasins ou les trains et les réseaux proposés par les universités, les accès WiFi d'entreprise proposés aux visiteurs et aux invités, les hotspots créés par des individus, etc.).

À cet égard, le GT29 souhaiterait que soit clarifié ce qu'il convient de considérer comme «accessible au public» ou non[9]. Seuls les services fournis dans le cadre d'une situation officielle ou professionnelle **exclusivement** à des fins professionnelles ou officielles, ou les communications techniques entre des organismes privés ou publics exclusivement en vue de contrôler les processus de travail ou commerciaux, ainsi que l'utilisation de services exclusivement à des fins domestiques, peuvent être exemptés de l'instrument «vie privée et communications électroniques». Le GT29 recommande que de tels exemples soient précisés à l'aide d'un considérant approprié afin de fournir orientations et clarté.

CONSÉQUENCES DES EXIGENCES DE CONSERVATION DES DONNÉES

En raison d'inquiétudes liées à l'imposition d'exigences de conservation des données non nécessaires ou injustifiées, le GT29 a jusqu'à présent hésité à imposer de telles obligations à un plus grand nombre de fournisseurs de services de communication. La directive 2006/24/CE (ci-après la «directive sur la conservation des données») ayant depuis lors été déclarée invalide par la CJUE[10], un obstacle important à l'inclusion d'autres acteurs que les fournisseurs publics de services de communications électroniques dans le champ d'application de l'instrument «vie privée et communications électroniques» révisé a été levé.

La Commission européenne devrait expressément déclarer qu'elle n'introduira pas de nouvelles exigences européennes de conservation des données. Toute conservation similaire de données de communication doit être interdite de façon générale dans l'instrument «vie privée et communications électroniques» révisé. La Commission européenne doit veiller à ce que l'extension du champ d'application du nouvel instrument «vie privée et communications électroniques» ne permette pas automatiquement aux États membres de faire entrer de nouveaux services de communication dans le champ d'application de législations nationales de conservation des données neuves ou existantes. En tout état de cause, il faut que le nouvel instrument «vie privée et communications électroniques» précise que toute législation nationale de conservation des données doit respecter les exigences de l'article 8 de la CEDH et de l'article 51, paragraphe 1, de la Charte.

3. PROTECTION DE LA CONFIDENTIALITÉ DES COMMUNICATIONS ÉLECTRONIQUES

La protection de la confidentialité des communications (article 5) est l'un des objectifs clés de l'actuelle directive «vie privée et communications électroniques». Il s'agit également de l'un des éléments essentiels de l'article 7 (respect de la vie privée et familiale), de l'article 8

[9] Par exemple, cette définition implique-t-elle l'impossibilité de prédire ou même de connaître l'identité des utilisateurs? Dans ce cas, exclut-elle les utilisateurs enregistrés par le service, ou, par exemple, les utilisateurs inscrits sur une liste d'invités?

[10] Cour de Justice de l'Union européenne, communiqué de presse nº 54/14. Luxembourg, 8 avril 2014, URL:https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054fr.pdf.

(protection des données à caractère personnel) et de l'article 11 (liberté d'expression et d'information) de la charte des droits fondamentaux de l'Union européenne. En outre, un certain nombre d'États membres de l'UE[11] reconnaissent le secret des communications comme un droit constitutionnel.

RÉVISION DE L'ARTICLE 5, PARAGRAPHE 1

Lors de la révision des règles de l'instrument «vie privée et communications électroniques», le nouvel instrument devrait maintenir l'interdiction générale de l'interception/de la surveillance/du suivi du contenu des communications électroniques.

La Commission européenne devrait également tenir compte de l'attente raisonnable des utilisateurs selon laquelle toute intrusion non autorisée dans leurs communications par le fournisseur des communications est interdite.

L'article révisé doit protéger les utilisateurs contre l'interception du contenu de leurs communications, qu'il s'agisse de communications électroniques directes entre utilisateurs ou au sein d'un groupe d'utilisateurs définis (par exemple, une conférence téléphonique ou un webcast), ainsi que contre le traitement de leurs données de communications. De telles communications devraient être protégées par le même degré de confidentialité que celles actuellement couvertes par le champ d'application de la directive «vie privée et communications électroniques», à l'exception des contenus traités par les utilisateurs concernés à des fins domestiques uniquement.

Le groupe de travail encourage donc la Commission européenne à étendre le champ d'application de l'article 5, paragraphe 1, à tout service aux fonctions équivalentes à celles des services et réseaux de communications électroniques. Ces services ont pour point commun qu'ils permettent l'échange de messages entre un nombre fini d'utilisateurs. **Pour ce faire, la Commission pourrait élargir la définition de «communication» établie à l'article 2, point d), afin d'inclure explicitement les «utilisateurs» tels que définis à l'actuel article 2, point a), de la façon suivante: «toute information échangée ou acheminée entre un nombre fini de parties ou d'utilisateurs».**

Afin d'éviter tout vide juridique dans la protection des utilisateurs, **la Commission devrait indiquer dans un considérant que l'interception et la surveillance devraient être interprétées selon leur signification technique la plus large, et y inclure l'attribution d'identifiants uniques tels que des identifiants publicitaires, des balises audio ou des super cookies aux communications (ou à leur contenu ou aux données relatives au trafic y afférentes)**.

Le groupe de travail recommande également de **clarifier les définitions des «données de communications» et des «données relatives au trafic y afférentes».** La formulation actuelle de l'article 5, paragraphe 1, de l'instrument «vie privée et communications électroniques» a semé une certaine confusion concernant la signification de l'interdiction d'interception ou de surveillance des «communications et des données relatives au trafic y afférentes» visée à l'article 5, paragraphe 1, ainsi que des règles distinctes applicables au traitement des données relatives au trafic à l'article 6. La distinction historique entre contenu et métadonnées n'est plus aussi évidente. Avec la simple téléphonie à l'ancienne, une distinction nette pouvait être

[11] Par exemple, l'Allemagne à l'article 10 de la Grundgesetz (secret des communications).

faite entre l'interception de l'appel lui-même et les données relatives au trafic (qui a appelé qui et quand).

Les communications numériques sont régies par des protocoles techniques qui ne différencient pas nécessairement le contenu des communications et les données relatives au trafic y afférentes. Par exemple, le protocole HTTP prescrit l'utilisation d'URL contenant à la fois des éléments de contenu (pages internet consultées dont le contenu peut être lu à partir de l'ancrage et des paramètres de l'URL) et des données relatives au trafic (noms d'hôtes). Il est donc de plus en plus difficile d'appliquer les définitions juridiques distinctes de données relatives au trafic et de données de communications, notamment lorsqu'un fournisseur de réseau procède à une inspection des paquets et que l'analyse révèle le contenu des communications entre les utilisateurs et des tiers (les URL consultées).

Le groupe de travail constate que la transposition de la législation relative à la conservation des données par les États membres a également entraîné des différences d'interprétation de ces définitions essentielles, donnant ainsi lieu à une incertitude réglementaire. Par conséquent, le groupe de travail invite la Commission à **illustrer, à l'aide d'exemples clairs, les cas où les règles de confidentialité applicables aux communications et aux données relatives au trafic y afférentes (actuellement définies à l'article 5, paragraphe 1, de la directive «vie privée et communications électroniques») doivent être respectées, et les cas où seules les règles spécifiques applicables aux données relatives au trafic doivent être respectées (actuellement définies à l'article 6 de la directive «vie privée et communications électroniques»**). Cette problématique est également pertinente lorsque les fournisseurs de réseaux de communication accessibles au public proposent eux-mêmes des services de communications accessibles au public (par exemple, téléphonie mobile, télévision numérique, paiement à l'utilisation et vidéos à la demande) et peuvent collecter et stocker des données liées à l'utilisation desdits services et révélant des informations relatives au contenu des communications, telles que les URL consultées. **Le groupe de travail recommande de fournir une liste exhaustive dans un considérant spécifique.**

De façon générale, la Commission européenne devrait préciser que les exigences du RGPD relatives à la limitation des finalités et à la minimisation des données s'appliquent. Le traitement du contenu des communications et des données relatives au trafic y afférentes ne peut être légitime que s'il est effectué à une fin légitime spécifique et si les catégories et le volume de données à traiter sont limités au minimum nécessaire à la fourniture du service demandé. En règle générale, même si une exception permettant l'interception de la communication s'applique, les données devraient être supprimées ou anonymisées de manière irréversible dès que possible. La Commission européenne doit fournir une explication (conformément à l'avis 5/2014 du GT29 sur les techniques d'anonymisation) indiquant clairement que les données ne sont pas anonymes tant que l'opérateur dispose toujours des données d'origine à une autre fin.

En outre, l'actuelle exception à l'exigence de consentement applicable aux «transactions commerciales licites» n'est pas suffisamment précise. Il doit être clair que l'utilisation des données à des fins de publicité, de marketing, d'«innovation de produits» ou de recherche ne devrait jamais pouvoir prévaloir sur l'exigence de consentement préalable à l'interception du contenu des communications et des données relatives au trafic y afférentes.

Afin de tenir compte de certaines utilisations légitimes des données de contenu, notamment lorsqu'il s'agit d'assurer le service fourni aux utilisateurs, la Commission pourrait créer les deux exceptions suivantes à l'exigence de consentement:

1. transmission: si les données sont, d'un point de vue technique, strictement nécessaires à la transmission de la communication électronique requise par un utilisateur. Il devrait être absolument clair que la distribution de publicité et l'utilisation des données à des fins de marketing, de recherche et de mesure d'audience ne sont pas considérées comme strictement nécessaires à la fourniture d'un service requis par un utilisateur;

2. sécurité: si le traitement est strictement nécessaire afin de maintenir et de gérer, de façon proactive et défensive, la sécurité d'un réseau ou d'un service (y compris l'établissement de prévisions concernant le réseau, la détection et la résolution de problèmes indirects ou structurels ou la détection, la résolution et la prévention de spams, de logiciels malveillants, de logiciels espions et de violations de données). Tout enregistrement de données de contenu doit être supprimé dès qu'il n'est plus nécessaire à cette fin.

La Commission devrait préciser que les exigences du RGPD relatives à la proportionnalité et à la subsidiarité s'appliquent dans tous les cas, que le consentement soit requis ou non, ou que l'une des exceptions soit invoquée ou non.

RÉVISION DE L'ARTICLE 5, PARAGRAPHE 3

Tout en conservant l'exigence de consentement définie à l'actuel article 5, paragraphe 3, de la directive «vie privée et communications électroniques», les règles devraient être reformulées afin de mieux protéger la confidentialité des dispositifs de communication des utilisateurs. La formulation actuelle de l'exigence de consentement pour «le stockage d'informations» ou «l'obtention de l'accès à des informations déjà stockées» dans l'équipement terminal (dispositifs de communication) des utilisateurs a créé une certaine ambiguïté quant à son applicabilité.

L'article 5, paragraphe 3, révisé devrait être reformulé de façon aussi neutre que possible sur le plan technologique. Les techniques de pistage utilisées sur les smartphones et les applications de l'internet des objets devraient être prises en compte dans la définition des actions couvertes par l'article 5, paragraphe 3, révisé, notamment en ce qui concerne le «pistage passif», c'est-à-dire l'utilisation d'identifiants et d'autres données transmises par les dispositifs. Par exemple, afin d'établir des communications avec un point d'accès WiFi, les smartphones transmettent en continu leur adresse MAC. Ces signaux peuvent être captés et traités à une autre fin que celle de procéder à la transmission d'une communication, par exemple en vue de compter les visiteurs, voire de déduire des profils de localisation détaillés au fil du temps et d'un endroit à l'autre. L'internet des objets a permis la transmission «par défaut» de toujours plus de données pour des raisons techniques, mais utilisées à des fins d'intrusion (notamment à des fins de marketing) sans lien avec la finalité initiale de cette transmission. Autrement dit, **les règles gouvernant la collecte d'informations à partir des dispositifs des utilisateurs ne devraient pas dépendre du type d'appareil détenu par la personne concernée ou de la technologie employée par une organisation**, notamment en ce qui concerne l'utilisation d'informations à des fins de marketing et d'analyse du marché.

La Commission européenne devrait également préciser que les données ne doivent pas

nécessairement être stockées dans l'équipement terminal, mais qu'elles peuvent également être traitées (y compris collectées et stockées) ailleurs et rendues disponibles au moyen de l'appareil, et que dans ces situations, l'article 5, paragraphe 3, s'applique. Toutefois, en clarifiant la vaste portée de l'exigence de consentement, la Commission devrait également définir des exceptions plus spécifiques afin de permettre le traitement de données ayant peu ou pas d'incidence sur le droit des utilisateurs au secret des communications et à la vie privée.

Le groupe de travail a déjà exhorté la Commission (avis 04/2012 sur l'exemption de l'obligation de consentement pour certains cookies) à créer une nouvelle exception pour les cookies d'analyse d'origine qui sont peu susceptibles de présenter «*un risque pour la vie privée lorsqu'ils sont strictement limités à l'établissement de statistiques agrégées concernant l'origine*». Une telle pratique est autorisée à condition que les sites internet fournissent «*des informations claires sur ces cookies dans leurs dispositions relatives à la protection de la vie privée, ainsi que des garanties adéquates en la matière*», telles qu'un «*dispositif facile à utiliser permettant de ne pas participer aux mécanismes de collecte de données et d'anonymisation intégrale qui sont appliqués à d'autres informations identifiables collectées telles que les adresses IP*»[12].

Au vu du développement et du déploiement rapides de nouvelles façons de pister les utilisateurs au moyen des informations stockées dans leurs appareils ou transmises par ceux-ci, l'exception ne devrait pas se limiter à une technique en particulier, mais se concentrer sur l'incidence sur la vie privée des utilisateurs et sur leur droit au secret des communications.

Il devrait exister au moins deux exceptions à l'exigence de consentement:

1. transmission (l'exemption actuelle devrait rester d'application) – si les données sont, d'un point de vue technique, strictement nécessaires à la transmission de la communication électronique requise par un utilisateur. Il devrait être absolument clair que la distribution de publicité et l'utilisation des données à des fins de marketing, de recherche et de mesure d'audience ne sont pas considérées comme strictement nécessaires à la fourniture d'un service requis par un utilisateur;

2. sécurité – si le traitement est strictement nécessaire afin de maintenir et de gérer, de façon proactive et défensive, la sécurité technique d'un réseau ou d'un service, y compris l'établissement de prévisions concernant le réseau, la détection et la résolution de problèmes indirects ou structurels (y compris afin de fournir un service client à cet égard) ou la détection, la résolution et la prévention de spams, de logiciels malveillants, de logiciels espions et de violations de données.

En outre, le groupe de travail invite la Commission à envisager d'autres circonstances dans lesquelles le consentement ne serait pas requis, dès lors que le traitement n'aurait que peu, voire aucun effet sur le droit des utilisateurs à la protection du secret de leurs communications et de leur vie privée.

De telles circonstances pourraient être les suivantes:

[12] En bref, le GT29 soutenait l'insertion d'un «troisième critère d'exemption de l'obligation de consentement pour les cookies strictement limités à l'établissement de statistiques anonymisées et agrégées concernant le domaine d'origine».

1. anonymisation – si les données sont immédiatement et irréversiblement anonymisées lors de leur collecte sur l'appareil, ou sur les extrémités du réseau/des capteurs. Il doit être clair que cette exception ne peut pas s'appliquer tant que le fournisseur du service, ou un tiers en collaboration avec lequel le fournisseur assure un service, a toujours accès aux données d'origine stockées à une autre fin. Le consentement serait alors toujours nécessaire si les données sont simplement hachées, agrégées ou pseudonymisées de toute autre façon, mais qu'il demeure possible de relier certains événements des données agrégées aux données d'origine, ainsi que si de futures lectures des informations tirées d'un appareil permettraient de créer un lien avec certains événements du jeu de données agrégé;

2. lorsque la collecte de données est conçue pour avoir une incidence limitée voire nulle sur le droit à la vie privée et à la confidentialité des communications. Cette exception ne peut être invoquée que dans les conditions (cumulatives) suivantes:

- la collecte de données est strictement limitée à l'analyse statistique de la qualité du service fourni par la personne physique ou morale, l'autorité publique, l'agence ou tout autre organe déterminant la finalité et les moyens du service («partie d'origine»)[13]. Si un tiers est impliqué dans la collecte technique des données, cette exception ne peut être invoquée que si ce tiers a signé un accord de sous-traitance tel que défini à l'article 28 du RGPD et si ledit accord interdit toute autre utilisation des données collectées par le sous-traitant à toute autre fin. Cette exception ne peut pas être invoquée pour l'analyse de données de localisation;
- la collecte a lieu dans une zone restreinte et unique. Cela exclut le pistage et le profilage des utilisateurs (fondés sur la collecte d'informations stockées sur leurs appareils ou transmises par ceux-ci) dans différents endroits et/ou domaines ou services;
- l'utilisateur dispose d'informations préalables et adéquates concernant la collecte et les finalités du traitement, telles que définies aux articles 12 à 14 du RGPD;
- un dispositif facile à utiliser permettant de ne pas participer aux mécanismes de collecte de données est proposé aux utilisateurs, sans engendrer de nouveaux risques pour le respect de leur vie privée;
- la collecte et le traitement des informations servent un objectif légitime et respectent les principes de proportionnalité et de subsidiarité, de sorte qu'ils sont conçus pour avoir une incidence limitée. En fonction des circonstances, cet objectif peut être atteint en utilisant des échantillons plutôt que l'ensemble du jeu de données, en veillant à ce que les catégories et le volume de données collectées soient limités au minimum nécessaire à cette fin spécifique et/ou en appliquant des mécanismes d'anonymisation intégrale aux données collectées après une période de temps limitée;
- les données traitées ne constituent pas des données de nature sensible et des catégories particulières de données à caractère personnel en vertu de l'article 9 du RGPD (y compris, par exemple, des données concernant des zones ou des partenaires de communication permettant de déduire des données sensibles).

Concernant la première exception, les informations fournies aux utilisateurs peuvent se limiter à une description générale de la finalité en question, mais pour ce qui est de la deuxième exception et des autres circonstances dans lesquelles le consentement ne serait pas requis, il convient que l'instrument «vie privée et communications électroniques» révisé précise que les

[13] Dans son avis sur l'exemption de l'obligation de consentement pour certains cookies (p. 12), le groupe de travail note: «*L'analytique d'origine doit être clairement distinguée de l'analytique de tiers, qui utilise un cookie tiers ordinaire pour collecter des informations de navigation liées à des utilisateurs sur des sites web distincts, et qui présente un risque nettement plus élevé pour le respect de la vie privée.*»

utilisateurs doivent être informés des catégories de données et des finalités du traitement.

Le groupe de travail souhaiterait une définition juridique claire des finalités du traitement des données qui ne nécessitent pas de consentement. En outre, le groupe de travail conseille à la Commission européenne de se référer à de futures orientations fournies par le comité européen de la protection des données.

FUSION DES ARTICLES 6 ET 9 (DONNÉES RELATIVES AU TRAFIC ET DONNÉES DE LOCALISATION)

Au-delà de la protection vis-à-vis des parties d'origine assurée à l'article 5, paragraphe 1, le champ d'application de l'article 5, paragraphe 3, est étendu à toutes les parties portant atteinte à la confidentialité des informations stockées sur l'appareil. Toutefois, les articles 6 et 9 de la directive «vie privée et communications électroniques» concernant le traitement des données relatives au trafic et des données de localisation ne s'appliquent, une fois encore, qu'aux fournisseurs «d'origine» traditionnels, et non aux autres parties traitant ces données.

La Cour de justice de l'Union européenne a reconnu dans des arrêts récents que les métadonnées des communications peuvent fournir un aperçu intrusif et révélateur des intérêts et de la localisation d'une personne. Or ces données ne sont plus uniquement collectées par des fournisseurs de téléphonie et de services internet traditionnels, mais également par de nombreuses autres organisations, y compris à l'extérieur de l'UE. Ces nouveaux fournisseurs de services, tels que les développeurs d'applications, peuvent également obtenir un aperçu très détaillé du profil de déplacement et de communication d'un utilisateur, sans nécessairement être soumis aux obligations de l'actuelle directive «vie privée et communications électroniques» (tant qu'ils ne lisent pas les informations stockées dans l'équipement terminal des utilisateurs). En outre, du fait de ces nouveaux services, la frontière entre les données relatives au trafic et les données de localisation s'est estompée.

L'observation récurrente des données de localisation permet de dégager des profils de déplacement, y compris des adresses personnelles et des adresses professionnelles. Les données relatives au trafic telles que le comportement téléphonique peuvent dévoiler des profils sociaux et des relations entre utilisateurs, tandis que les données relatives au trafic sur internet peuvent révéler l'orientation sexuelle, ou l'affiliation politique par exemple.

Même si certains pans des données de communication sont immédiatement supprimés du jeu de données après leur collecte, la collecte de données relatives au trafic et de données de localisation au fil du temps et/ou sur différentes plateformes/différents domaines/différents services peut permettre d'élaborer des profils individuels ou des profils de groupe, ou encore des statistiques pouvant être exploitées pour procéder à un traitement différencié des utilisateurs. Les pistages de ce type ont donc une incidence élevée sur la vie privée des utilisateurs et justifient la nécessité d'un consentement préalable.

En fusionnant les dispositions de l'actuelle directive qui concernent les données relatives au trafic et les données de localisation, l'instrument «vie privée et communications électroniques» révisé pourrait définir une règle claire applicable à toutes les parties. En exigeant un consentement pour le traitement de toutes ces métadonnées, l'instrument «vie privée et communications électroniques» révisé assurera un niveau de protection élevé s'appuyant sur le fondement juridique fort qu'est le consentement de la personne concernée, visé à l'article 6 du RGPD. La confidentialité des communications est un droit fondamental

pour toute société démocratique. Aussi la confidentialité des communications et des métadonnées y afférentes nécessite-t-elle des règles plus strictes, notamment parce que les technologies de communication modernes permettent la collecte massive de données intrusives à l'aide de techniques secrètes, ou du moins de techniques dont les citoyens ne sont pas entièrement conscients. La collecte, le traitement et l'utilisation de ces données à d'autres fins que celle d'assurer la communication requise doivent être exceptionnels et uniquement autorisés si les utilisateurs ont été informés de façon appropriée et ont donné leur consentement.

Afin de mieux protéger le secret des communications électroniques, le groupe de travail recommande donc à la Commission européenne de définir une exigence de consentement harmonisée pour le traitement des métadonnées telles que les données relatives au trafic et les données de localisation. Cette exigence de consentement devrait s'appliquer à l'ensemble des données relatives au trafic et des données de localisation, y compris lorsqu'elles sont générées par des capteurs dans l'appareil d'un utilisateur. Cette nouvelle règle devrait s'appliquer à toutes les parties qui collectent et traitent ces données.

La définition du consentement est actuellement fournie par la directive 95/46/CE, conformément à l'article 2 de la directive «vie privée et communications électroniques». Le nouvel instrument «vie privée et communications électroniques» devrait également utiliser la définition du consentement de la personne concernée énoncée au considérant 32 et à l'article 4, paragraphe 11, du RGPD et respecter les conditions décrites à son considérant 42 et à son article 7, notamment en ce qui concerne sa forme ainsi que la capacité du responsable du traitement à prouver un tel consentement. En clarifiant la vaste portée de l'exigence de consentement pour les données relatives au trafic et les données de localisation, la Commission devrait également définir des exceptions plus spécifiques afin de permettre le traitement de données ayant peu ou pas d'incidence sur le droit des utilisateurs au secret des communications et à la vie privée.

Comme le groupe de travail l'a indiqué dans son avis 04/2012, tous les usages de la technologie relevant du champ d'application de l'article 5, paragraphe 3, ne présentent pas un risque pour le respect de la vie privée des utilisateurs. De la même façon, lorsque les opérateurs de réseau et les fournisseurs de services traitent les données relatives au trafic et les données de localisation nécessaires afin de fournir, sur le plan technique, un service requis (uniquement à cette fin), un tel traitement ne présente pas nécessairement un risque élevé pour les utilisateurs. D'autres exemples pertinents de traitement présentant un risque peu élevé pour le respect de la vie privée des utilisateurs sont le traitement à des fins de facturation et à des fins de sécurité spécifiques, telles que la détection de logiciels malveillants, de spams, de réseaux zombies, de fraudes ou de violations de données, à condition que ce traitement respecte les exigences de transparence et de proportionnalité et que des garanties appropriées soient en place afin de protéger les droits et les intérêts des personnes concernées.

Conformément à cette approche consistant à distinguer les finalités en fonction de l'incidence qu'elles ont sur les droits des utilisateurs, il devrait exister au moins trois exceptions à l'exigence de consentement:

1. transmission – si les données sont, d'un point de vue technique, strictement nécessaires à la transmission de la communication électronique requise par un utilisateur. Il devrait être absolument clair que la distribution de publicité et l'utilisation des données à des fins de

marketing, de recherche et de mesure d'audience ne sont pas considérées comme nécessaires à la fourniture d'un service requis par un utilisateur;

2. sécurité – si le traitement est strictement nécessaire afin de maintenir et de gérer, de façon proactive et défensive, la sécurité d'un réseau ou d'un service [y compris l'établissement de prévisions concernant le réseau, la détection et la résolution de problèmes indirects ou structurels (également afin de fournir un service client à cet égard) ou la détection, la résolution et la prévention de fraudes, de spams, de logiciels malveillants, de logiciels espions et de violations de données];
3. facturation – si le traitement des données relatives au trafic et des données de localisation est strictement nécessaire à la facturation/aux transactions électroniques ou pour garder une trace de ces dernières. Cette exception ne devrait pas permettre aux parties d'envoyer des factures pour des services «gratuits» afin de traiter des données qui nécessiteraient autrement le consentement des utilisateurs.

En outre, le groupe de travail invite la Commission à envisager d'autres circonstances dans lesquelles le consentement ne serait pas requis, dès lors que le traitement n'aurait que peu, voire aucun effet sur le droit des utilisateurs à la protection du secret de leurs communications et de leur vie privée.

De telles circonstances pourraient être les suivantes:

1. anonymisation – si les données sont immédiatement supprimées ou irréversiblement anonymisées après la transmission d'une communication. Il doit être clair que cette exception ne peut pas être invoquée tant que le fournisseur du service, ou un tiers en collaboration avec lequel le fournisseur assure un service, a toujours accès aux données d'origine stockées à une autre fin. Le consentement serait alors toujours nécessaire si les données sont simplement hachées, agrégées au niveau des événements ou pseudonymisées de toute autre façon, mais qu'il demeure possible d'identifier des utilisateurs ou de relier certains événements des données agrégées aux données d'origine, ainsi que si de futures collectes de données relatives au trafic ou de données de localisation permettraient de créer un lien avec certains événements du jeu de données agrégé;
2.
3. lorsque la collecte de données et leur traitement (complémentaire) sont conçus pour avoir une incidence limitée voire nulle sur le droit à la vie privée et à la confidentialité des communications. Cette exception ne peut être invoquée que dans les conditions (cumulatives) suivantes:
4. l'utilisateur dispose:
5. d'informations préalables et adéquates concernant la collecte et les finalités du traitement, telles que définies aux articles 12 à 14 du RGPD;
6. concernant les données de localisation: d'un dispositif facile à utiliser permettant de ne pas participer aux mécanismes de collecte de données;
7. la collecte et le traitement des informations servent un objectif légitime et respectent les principes de proportionnalité et de subsidiarité, de sorte qu'ils sont conçus pour avoir une incidence limitée. En fonction des circonstances, cet objectif peut être atteint en utilisant des échantillons plutôt que l'ensemble du jeu de données, en veillant à ce que les catégories et le volume de données collectées soient limités au minimum nécessaire à cette fin spécifique et/ou en appliquant des mécanismes d'anonymisation intégrale aux

données collectées après une période de temps qui devrait être limitée à la période strictement nécessaire;

8. les données traitées ne constituent pas des données de nature sensible ou des catégories particulières de données à caractère personnel en vertu de l'article 9 du RGPD (par exemple des données concernant des zones ou des partenaires de communication permettant de déduire des données sensibles).

Concernant la deuxième et la troisième exception, ainsi que d'autres circonstances dans lesquelles le consentement ne serait pas requis, il faut que l'instrument «vie privée et communications électroniques» révisé précise que les utilisateurs doivent être informés des données et des finalités du traitement.

Une fois que les dispositions concernant les données relatives au trafic et les données de localisation auront été fusionnées, les actuelles exceptions spécifiques concernant le marketing et les «services à valeur ajoutée» ne seraient plus nécessaires.

CONSIDÉRATIONS CONCERNANT LE CONSENTEMENT DE L'UTILISATEUR EXIGÉ DANS L'INSTRUMENT «VIE PRIVÉE ET COMMUNICATIONS ÉLECTRONIQUES»

Le GT29 a fourni des orientations détaillées relatives à l'exigence de consentement en ce qui concerne les cookies et les technologies similaires dans son avis 04/2012[14], dans son document de travail 02/2013[15] et dans son avis 9/2014[16]. Il a également fourni des orientations générales sur le consentement lui-même dans son avis 15/2011[17].

Le consentement préalable de l'utilisateur devrait demeurer un principe clé dans le nouvel instrument «vie privée et communications électroniques» concernant la collecte de métadonnées et de données de contenu ainsi que les techniques de pistage. Afin d'assurer la cohérence avec le RGPD, le nouvel instrument devrait clairement faire référence aux dispositions de ce dernier, en précisant la définition, les conditions et les formes de consentement.

D'une part, étant donné la nature sensible des données de communications, le consentement constitue le fondement juridique privilégié pour permettre aux utilisateurs de déterminer, grâce à des informations adéquates, s'ils autorisent le traitement envisagé à une fin spécifique. D'autre part, le GT29 constate que dans de nombreux cas, l'industrie a développé des mécanismes de consentement censés lui permettre de se conformer aux exigences juridiques minimales, mais qui ne permettent pas aux utilisateurs de procéder à un choix véritablement libre concernant ce traitement. C'est notamment le cas de ce que l'on appelle les «cookie walls» (ou «accès subordonné à l'acceptation de témoins de connexion»). Dans la pratique,

[14] GT29, WP 194, avis 04/2012 sur l'exemption de l'obligation de consentement pour certains cookies, URL:https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_fr.pdf.
[15] GT29, WP 208, document de travail 02/2013 énonçant des lignes directrices sur le recueil du consentement pour le dépôt de cookies, URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp208_fr.pdf
[16] GT29, WP 224, avis 9/2014 sur l'application de la directive 2002/58/CE à la capture d'empreintes numériques, URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp224_fr.pdf
[17] GT29, WP 187, avis 15/2011 sur la définition du consentement, URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_fr.pdf

ces mécanismes entraînent le refus d'accès au site concerné pour les utilisateurs qui n'acceptent pas les cookies, y compris lorsqu'il s'agit de cookies de pistage à finalité commerciale présentant un risque élevé pour le respect de la vie privée des utilisateurs.

Ces approches de type «à prendre ou à laisser» respectent rarement l'exigence d'un consentement donné librement, tel que défini dans la directive 95/46/CE et en particulier au considérant 43 du RGPD. Dans son avis sur le consentement, le GT29 indiquait spécifiquement que «*si les conséquences du consentement sapent la liberté de choix des personnes, le consentement n'est pas libre*». Le groupe de travail invite la Commission à développer une interdiction spécifique de ces choix de type «à prendre ou à laisser» concernant les communications électroniques lorsque de tels choix saperaient le principe de consentement donné librement.

Le groupe de travail a recensé cinq circonstances dans lesquelles le consentement forcé devrait être spécifiquement interdit et dans lesquelles les utilisateurs devraient être libres de choisir d'accepter et de refuser le traitement de leurs données tout en étant en mesure d'utiliser le service, à savoir:

1. le pistage sur des sites internet, des applications ou des emplacements qui révèlent des informations relatives à des catégories particulières de données (santé, informations à caractère politique, sexuel, syndical, etc.). Même si la consultation de services fournissant des informations relatives à de telles catégories particulières de données ne révèle pas en elle-même des catégories particulières de données au sujet des utilisateurs concernés, si ces derniers sont considérés comme étant intéressés par de telles informations, l'incidence sur leur vie privée serait élevée;

2. le pistage par des tiers non identifiés à des fins non spécifiées. C'est notamment le cas lorsqu'un site internet ou une application met aux enchères son espace publicitaire et que des tiers non identifiés peuvent effectivement commencer à pister les utilisateurs par l'intermédiaire du site internet ou de l'application en question;

3. tous les services financés par le gouvernement;

4. toutes les circonstances entraînant l'invalidité du consentement telles que déterminées dans le RGPD, par exemple un déséquilibre du rapport de force, l'absence d'alternative ou l'intégration d'un consentement forcé dans un contrat;

5. un consentement groupé pour le traitement des données à plusieurs fins. Le consentement devrait être détaillé.

Le groupe de travail exhorte la Commission à accorder une attention particulière aux médias d'information, dès lors qu'ils semblent être les plus grands utilisateurs de cookies de pistage et de «cookie walls»[18]. Assurer la survie économique des médias d'information constitue une nécessité démocratique évidente. La Commission européenne ne devrait cependant pas accepter que les médias d'information imposent un pistage intrusif des utilisateurs.

[18] Recherches récentes de Steven Englehardt et Arvind Narayanan de l'université de Princeton, Online tracking: A 1-million-site measurement and analysis. Rédaction: 18 mai 2016. Voir par exemple le lien suivant: http://motherboard.vice.com/read/news-sites-are-tracking-your-web-traffic-way-more-than-porn-sites.

Lorsque le consentement est le fondement juridique applicable, les utilisateurs doivent disposer de moyens réellement simples (faciles à utiliser) pour octroyer et retirer leur consentement. **Le groupe de travail recommande de reformuler les exigences décrites dans l'actuel considérant 66 de la directive 2009/136/CE. Au lieu de s'en remettre aux opérateurs de sites internet pour obtenir le consentement des utilisateurs au nom de tiers** (par exemple, publicités et réseaux sociaux), les fournisseurs de **navigateurs et autres logiciels ou systèmes d'exploitation devraient être encouragés à développer, à mettre en œuvre et à assurer une responsabilisation effective des utilisateurs en proposant des outils de contrôle intégrés au navigateur** (ou à d'autres logiciels ou systèmes d'exploitation), tels que des outils d'interdiction du suivi (Do Not Track ou DNT), ou d'autres moyens techniques qui permettent aux utilisateurs d'exprimer et de retirer facilement leur consentement spécifique, conformément à l'article 7 du RGPD. De tels outils peuvent être proposés à l'utilisateur lors de la configuration initiale, avec des paramètres par défaut favorables au respect de la vie privée. Le respect des normes techniques et de conformité reconnues doit devenir une pratique courante. En outre, les opérateurs de sites internet devraient respecter et adopter les outils de contrôle intégrés aux navigateurs ou d'autres paramètres de préférences de l'utilisateur.

4. PROTECTION DE LA SÉCURITÉ DES COMMUNICATIONS ÉLECTRONIQUES

L'objectif principal de l'article relatif à la sécurité de l'instrument «vie privée et communications électroniques» révisé (actuellement l'article 4 de la directive «vie privée et communications électroniques») ne devrait pas uniquement être de protéger la sécurité (et en particulier la confidentialité) des communications lors de leur transmission ou de leur stockage, mais également de protéger la sécurité de l'équipement de l'utilisateur final. Cet objectif devrait être précisé dans le texte de la législation et pas uniquement dans un considérant (actuellement le considérant 24 de la directive «vie privée et communications électroniques»). Le groupe de travail recommande d'inclure une référence directe aux obligations du RGPD en matière de sécurité (telles que définies dans ses articles 5 et 32).

La Commission européenne devrait évaluer avec soin si les exigences de consentement élargies de l'instrument «vie privée et communications électroniques» révisé n'empêchent pas le traitement légitime à des fins de sécurité nécessaires[19].

L'article relatif à la sécurité, tel que révisé, devrait aussi spécifiquement protéger les appareils des utilisateurs finaux contre les logiciels espions (accès malveillant et non sollicité à des données de communication stockées sur l'appareil ou générées par celui-ci, ou stockage d'informations sur l'appareil d'un utilisateur final, y compris le préchargement de logiciels ou les informations push non sollicitées).

[19] Par exemple, le groupe de travail «Article 29» a déjà estimé dans son avis 1/2009 que les fournisseurs de courriers électroniques peuvent utiliser des systèmes de filtrage afin de détecter des virus, étant donné leur obligation de prendre des mesures d'ordre technique et organisationnel appropriées afin de garantir la sécurité de leurs services, conformément à l'obligation de sécurité prévue à l'article 4 de la directive «vie privée et communications électroniques».

Le groupe de travail est favorable à l'inclusion des propositions suivantes issues de la consultation publique sur l'évaluation et la révision de la directive «vie privée et communications électroniques» de la Commission européenne[20]:

- 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. Par exemple, les mises à jour obligatoires sont autorisées, mais l'utilisateur devrait être informé de façon adéquate au sujet des nouveaux risques en matière de sécurité et être en mesure de mettre facilement le système d'exploitation à jour par lui-même;
- extension des exigences en matière de sécurité afin d'élargir la couverture de l'internet des objets tels que ceux utilisés dans les dispositifs informatiques portables («wearable computing»), la domotique, la communication de véhicule à véhicule; 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 des signaux, etc.[21]

Le groupe de travail invite également la Commission européenne à fournir des orientations supplémentaires concernant la mise en œuvre des principes essentiels de protection des données dès la conception et de protection des données par défaut tels que référencés au considérant 78 du RGPD[22].

Les principes de protection des données dès la conception et de protection des données par défaut devraient également s'appliquer aux fournisseurs de réseau, de composants de réseau et d'équipements terminaux (y compris l'internet des objets) ou complémentaires (y compris les logiciels) utilisés en combinaison avec la fourniture de services de communications électroniques[23]. Lors de la mise en œuvre des principes de protection des données dès la conception et de protection des données par défaut, les différentes parties devraient privilégier

[20] Commission européenne, consultation publique sur l'évaluation et la révision de la directive «vie privée et communications électroniques», URL: https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-eprivacy-directive.

[21] Voir également le rapport de la commission américaine du commerce (2016): «ASUS settles FTC charges that insecure home routers and "cloud" services put consumer's privacy at risk». 23 février 2016, URL: https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put.

[22] Ce considérant dispose que «*lors de l'élaboration, de la conception, de la sélection et de l'utilisation d'applications, de services et de produits qui reposent sur le traitement de données à caractère personnel ou traitent des données à caractère personnel pour remplir leurs fonctions, il convient d'inciter les fabricants de produits, les prestataires de services et les producteurs d'applications à prendre en compte le droit à la protection des données lors de l'élaboration et de la conception de tels produits, services et applications et, compte dûment tenu de l'état des connaissances, à s'assurer que les responsables du traitement et les sous-traitants sont en mesure de s'acquitter des obligations qui leur incombent en matière de protection des données. Les principes de protection des données dès la conception et de protection des données par défaut devraient également être pris en considération dans le cadre des marchés publics*».

[23] La normalisation constitue une réponse concrète aux questions pratiques soulevées par la mise en œuvre du mécanisme de consentement et de choix concernant le pistage sur internet (article 5, paragraphe 3) et la collecte de données relatives au trafic et de données de localisation (article 5, paragraphe 1, et articles 6 et 9), d'après les travaux du W3C et du GT29 concernant les spécifications de conformité DNT.

la mise en place de choix détaillés, permettant ainsi aux citoyens de recourir à une option de type «ne pas collecter» pour planifier ou désactiver rapidement toute collecte de données, ainsi que sur la prévention du suivi de la localisation (par exemple en désactivant les interfaces sans fil lorsqu'elles ne sont pas utilisées ou en utilisant des numéros d'identification aléatoires) afin de permettre la transparence et le contrôle de l'utilisateur et de limiter autant que possible la quantité de données tirées des appareils en transformant les données brutes en données agrégées directement sur l'appareil.

En outre, **le groupe de travail invite la Commission européenne à envisager de protéger le droit des utilisateurs à recourir à des mécanismes de chiffrement afin de protéger leurs communications électroniques.** Une telle règle pourrait aussi inclure l'élaboration de normes techniques de chiffrement, en vue d'appuyer également les exigences de sécurité revues dans le RGPD. 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. Mais dans le même temps, les gouvernements s'efforcent de trouver de nouvelles façons d'accéder aux communications chiffrées. Le groupe de travail souhaiterait que soient instaurées de nouvelles obligations relatives à l'utilisation d'algorithmes et de normes ayant démontré leur fiabilité en vue de protéger la confidentialité des communications chiffrées et d'interdire le déchiffrement, l'ingénierie inverse ou toute autre méthode de suivi de ces communications protégées par chiffrement, avec une description limitative des exceptions.

5. SUPPRESSION DE RÈGLES SPÉCIFIQUES RELATIVES À LA VIOLATION DES DONNÉES

Le GT29 recommande de supprimer les paragraphes 2 et 3 de l'article 4 de l'actuelle directive «vie privée et communications électroniques». Le RGPD impose déjà à tous les responsables du traitement, y compris les fournisseurs de services de communications électroniques accessibles au public, de notifier les violations de données à caractère personnel aux abonnés et aux autorités nationales compétentes (sous réserve de certaines exceptions). Pour éviter les doublons, le processus doit être simplifié et toutes les violations de données impliquant des données à caractère personnel devraient être communiquées aux autorités de contrôle prévues dans le RGPD, en utilisant les seuils de déclenchement définis dans cet instrument.

6. HARMONISATION DES DISPOSITIONS RELATIVES AUX COMMUNICATIONS NON SOLLICITÉES

Les règles actuelles de la directive «vie privée et communications électroniques» concernant les communications non sollicitées visent à protéger les utilisateurs contre les désagréments et les coûts causés par la réception de telles communications non sollicitées.

Les moyens empruntés pour procéder à ces communications non sollicitées ont évolué depuis l'entrée en vigueur de la directive. Par exemple, une communication non sollicitée peut débuter avec un automate d'appel, 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 GT29 recommande donc que les règles relatives aux communications non sollicitées soient reformulées afin de tenir compte des progrès récents. L'article 13 de l'instrument «vie privée et communications électroniques» tel que révisé devrait exiger le consentement préalable des destinataires pour tous les types de communications non sollicitées, quels que soient les moyens empruntés (par exemple, courrier électronique, publicité comportementale, appels vocaux ou vidéo, fax, messages texte et messagerie ciblée). La charge de la preuve de l'obtention du consentement (des personnes physiques ou morales) devrait incomber à l'émetteur ou au commanditaire de la communication non sollicitée, y compris la conservation de copies horodatées des informations fournies aux utilisateurs lors de l'obtention de leur consentement.

Les utilisateurs doivent être en mesure de retirer facilement et gratuitement un tel consentement par des moyens simples devant être indiqués lors de chaque communication ultérieure. Le destinataire devrait pouvoir retirer son consentement à tout moment et sans en indiquer la raison. Conformément à l'article 7, paragraphe 3, du RGPD, il devrait être aussi simple de retirer que de donner son consentement. Toute finalité commerciale de la communication devrait être clairement identifiée au début de la communication.

Les utilisateurs doivent être en mesure d'exprimer et de retirer leur consentement pour tous les secteurs ou pour des secteurs spécifiques de manière simple et ergonomique. Ils devraient, dans la mesure du possible, pouvoir le faire via leur navigateur ou tout autre logiciel ou système d'exploitation. Au vu des limites de l'expression et du retrait du consentement au cas par cas, le groupe de travail recommande la création de registres ou d'autres systèmes fournissant une solution effective de retrait facile du consentement ou de réajustement des préférences en matière de marketing pour toute une série d'organisations ou de secteurs spécifiques. Afin de refléter pleinement l'article 7, paragraphe 3, du RGPD, il est particulièrement important de mettre en place un mécanisme de guichet unique pour le retrait du consentement vis-à-vis du marketing tiers lorsque les coordonnées de la personne concernée ont été intégrées à des listes de marketing vendues à un grand nombre de tiers non identifiés.

Conformément à l'article 7 du RGPD, le consentement doit être spécifique. Si le consentement est sollicité pour l'inclusion des coordonnées dans des listes de marketing qui seront utilisées par des tiers, un tel consentement ne peut être légalement valable que s'il est distinct du consentement aux communications tierces, et non combiné à celui-ci. Les catégories de produits pour lesquelles des communications électroniques peuvent être envoyées et les (catégories de) destinataires doivent être clairement définis avant l'obtention du consentement[24]. Cette exigence s'applique également aux communications dites «hébergées», dans le cadre desquelles une organisation envoie une communication non sollicitée au nom d'autres organisations (par exemple, un e-mail ou des publicités ciblées sur les réseaux sociaux).

En outre, l'exception énoncée à l'article 13, paragraphe 2, de l'actuelle directive «vie privée et communications électroniques» pour les clients existants devrait être limitée à un niveau de communications de marketing raisonnable. Les parties ne devraient pas être autorisées à bombarder les utilisateurs d'un nombre excessif d'appels ou de messages de marketing. Par

[24] Conformément à l'avis 4/2010 WP 174 du GT29 sur le code de conduite européen de la FEDMA relatif à l'exploitation de données à caractère personnel dans le cadre d'opérations de marketing direct.

ailleurs, la définition et le champ d'application des «produits et services similaires» gagneraient à être clarifiés.

7. HARMONISATION DES DISPOSITIONS RELATIVES AUX ANNUAIRES D'ABONNÉS

L'article 12 de la directive «vie privée et communications électroniques» confère le droit aux abonnés de «*décider si les données à caractère personnel les concernant [...] doivent figurer dans un annuaire public [imprimé ou électronique]*». La formulation de cet article fait référence à une époque où des exemplaires papier des annuaires téléphoniques étaient distribués dans tous les foyers et où les citoyens faisaient appel à des services de renseignements téléphoniques. Cette formulation est source d'insécurité juridique pour ce qui est de savoir si le champ d'application de cet article couvre les services équivalents des réseaux sociaux ou d'autres services de la société de l'information.

Il convient dès lors de moderniser et de clarifier cet article. Étant donné la prédominance des services de réseautage et de messagerie dans la société d'aujourd'hui, le GT29 recommande d'inclure tous les types de services d'annuaires dans le champ d'application de l'instrument, en plus des types de services dont le rôle est simplement de consolider les annuaires d'autres services. En outre, l'exigence de consentement pour les «recherches inverses» prévue à l'actuel article 12, paragraphe 3, devrait s'appliquer explicitement à d'autres identificateurs de service, tels qu'une adresse électronique ou un nom d'utilisateur.

8. IDENTIFICATION DE LA LIGNE APPELANTE

La directive «vie privée et communications électroniques» confère aux destinataires d'appels le droit essentiel d'être informés de l'identité de l'appelant et de prendre des mesures contre les appels qui empêchent la présentation de l'identification de la ligne appelante. Certains États membres ont également renforcé la protection des citoyens à cet égard en adoptant des législations prescrivant que tous les appels de marketing sortants doivent afficher une identification de la ligne appelante valide[25]. Il est important de veiller au maintien de l'intégrité des informations d'identification de la ligne appelante transmises entre des réseaux interconnectés, de sorte que le souhait de l'utilisateur concernant l'affichage ou la dissimulation de l'identification de la ligne appelante soit respecté et que cette dernière ne puisse pas être usurpée ou falsifiée.

Le groupe de travail recommande une reformulation de l'article 8 de l'instrument «vie privée et communications électroniques» afin de tenir compte de ces évolutions.

9. APPLICATION

Afin de favoriser une interprétation harmonisée, le RGPD impose de nouvelles obligations

[25] Par exemple, au Royaume-Uni, la loi nº 10 sur les communications électroniques (Regulation 10 of the Privacy and Electronic Communications Regulations) (mettant en œuvre la directive «vie privée et communications électroniques au Royaume-Uni), URL: http://www.legislation.gov.uk/uksi/2003/2426/regulation/10/made

aux autorités de contrôle, telles que la coopération entre les autorités nationales compétentes, le mécanisme de contrôle de la cohérence et le rôle du comité européen de la protection des données.

L'actuelle directive «vie privée et communications électroniques» autorise les situations où plusieurs organes administratifs peuvent agir en qualité d'autorité de contrôle compétente. Les dispositions du nouvel instrument relatives au contrôle devraient, en tout état de cause, définir un modèle de gouvernance homogène prévoyant des mécanismes de coopération efficaces entre les différentes autorités de contrôle. En outre, dans les cas où plusieurs organes administratifs peuvent agir en qualité d'autorité de contrôle compétente, les sanctions devraient être harmonisées afin de correspondre à celles définies par le RGPD.

Dans la pratique, ces situations comprendront en général également le traitement de données à caractère personnel, entraînant un chevauchement en termes de contrôle. Le groupe de travail recommande donc à la Commission européenne d'établir que les autorités nationales de protection des données sont les autorités compétentes en ce qui concerne le nouveau cadre «vie privée et communications électroniques» afin d'assurer une réglementation et une application cohérentes et coordonnées.