Recommandations du CEPD concernant des aspects particuliers de la proposition de règlement «vie privée et communications électroniques»

5 octobre 2017

Une fois adoptée, la proposition de règlement «vie privée et communications électroniques» mettra à jour les «règles de conduite» en matière de respect de la vie privée et de communications électroniques. Le règlement modernisera les principes existants, clarifiera les exigences technologiques et prévoira une application efficace de ses dispositions. Le CEPD a publié sa position sur la révision de la directive «vie privée et communications électroniques» dans un avis préliminaire (5/2016) et sur la proposition de règlement de la Commission européenne dans son avis 6/2017. Compte tenu des développements intervenus dans les délibérations relatives à la proposition et à l'intention du colégislateur, le CEPD a décidé de présenter des recommandations et des clarifications sur quelques aspects spécifiques, dans le droit fil de ses avis antérieurs[1]. Les présentes recommandations insistent sur la nécessité de garantir la sécurité juridique et un niveau élevé de protection des droits fondamentaux au respect de la vie privée et à la protection des données.

Messages clés

- Le règlement «vie privée et communications électroniques» devrait refléter **l'importance du principe de confidentialité des communications**, qui est étroitement lié au droit au respect de la vie privée et, en tant que tel, est protégé par la Charte des droits fondamentaux de l'UE, la convention européenne des droits de l'homme et les ordres juridiques et constitutionnels de la plupart des États membres. La confidentialité des communications **couvre tout à la fois le contenu, les métadonnées et les données liées à l'équipement terminal.** Ceci devrait être dûment reflété dans les finalités de traitement autorisées et dans la base juridique du traitement. **Ces considérations s'appliquent à l'ensemble des dispositions du règlement «vie privée et communications électroniques».**

- Le règlement «vie privée et communications électroniques» devrait prévoir une véritable protection conforme aux développements technologiques actuels et attendus, notamment dans le contexte des **communications de machine à machine**. Le CEPD est donc favorable aux amendements qui prévoient expressément la protection de la confidentialité des communications pour les «*données **liées** aux équipements terminaux **ou traitées** par ceux-ci*». La confidentialité des communications devrait également être assurée lorsque des données **sont stockées dans le nuage** plutôt que seulement lors de leur transmission.

- Il convient de maintenir l'approche selon laquelle **le règlement «vie privée et communications électroniques» précise et complète le RGPD** afin de traduire

Adresse postale: rue Wiertz 60 - B-1047 Bruxelles
Bureaux: rue Montoyer 30
Adresse électronique: edps@edps.europa.eu - Site Internet: www.edps.europa.eu
Tél: 02-283 19 00 - Télécopie: 02-283 19 50

l'importance de la confidentialité des communications. **Le règlement «vie privée et communications électroniques» ne devrait pas abaisser le niveau de protection prévu dans le RGPD. Au contraire, un niveau de protection supérieur à celui offert par le RGPD devrait être mis en place.** Parallèlement, il convient d'éviter de répéter inutilement des dispositions du RGPD dans un souci de clarté et de sécurité juridique; en effet, reproduire de manière sélective certaines dispositions du RGPD risque d'aboutir à l'omission de dispositions importantes[2].

- Une large base juridique pour le traitement des données de communications faisant référence au RGPD ou reformulant le RGPD porterait atteinte à la raison d'être d'un instrument juridique spécifique et ne refléterait pas adéquatement l'importance de la confidentialité des communications consacrée à la fois par la Charte des droits fondamentaux de l'UE et par la jurisprudence de la CJUE et de la CouEDH. **En particulier, le règlement «vie privée et communications électroniques» ne devrait pas prévoir la possibilité d'un traitement des métadonnées fondé sur l'intérêt légitime.** Autoriser un traitement sur la base d'un intérêt légitime abaisserait de manière significative les normes actuellement en vigueur au titre de la directive 2002/58/CE «vie privée et communications électroniques» et remettrait en cause la valeur ajoutée du projet de règlement. De même, **un traitement ultérieur de métadonnées créerait une faille** et permettrait de contourner le niveau élevé de protection requis. **Les données liées à l'équipement terminal ne devraient être traitées qu'avec le consentement de l'utilisateur ou si le traitement est techniquement nécessaire pour un service demandé par l'utilisateur et uniquement pour la durée nécessaire à cette fin.** Le CEPD est donc favorable aux amendements qui suppriment la large base juridique pour le traçage des personnes physiques dans le temps et l'espace quelle qu'en soit la finalité.

- Des définitions appropriées sont indispensables pour mettre en œuvre la protection des droits fondamentaux. Le CEPD est donc favorable aux amendements qui prévoient des **définitions indépendantes**, remplaçant la référence au code des communications électroniques européen et veillant à ce que la personne physique qui utilise le service et/ou l'équipement technique donne son consentement lorsqu'une entité légale s'abonne au service. Le CEPD soutient également le fait que les services servant simplement de fonctions accessoires devraient être inclus dans la définition des «services de communications interpersonnelles». Enfin, le CEPD recommande fortement que la définition des métadonnées n'exclue pas les données qui ne sont pas nécessaires à la transmission du contenu de communications électroniques ou à la fourniture du service. De cette façon, aucune faille n'est créée pour le traitement de ces données fondé sur le RGPD.

- **Le consentement visé dans le règlement «vie privée et communications électroniques» doit avoir la même signification que dans le RGPD, notamment le fait qu'il doit être donné librement et spécifique.**
    - Le CEPD est dès lors favorable aux amendements précisant que toutes les dispositions du RGPD, notamment son article 4, paragraphe 11, sur la définition du consentement et ses articles 7 et 8 s'appliquent également aux fins du règlement «vie privée et communications électroniques».

    - Le CEPD soutient les amendements qui précisent que l'**accès aux services et aux fonctionnalités ne doit pas être subordonné au consentement au traitement** de données à caractère personnel et au traitement d'informations liées à l'équipement terminal des utilisateurs finaux ou traitées par celui-ci.

- Il se félicite également des amendements exigeant que les **paramètres techniques permettant le contrôle de l'utilisateur au titre de l'article 9 offrent une granularité suffisante.** Cette exigence reflète la règle du RGPD, qui veut qu'un consentement spécifique soit donné à des fins précises et pour des responsables spécifiques du traitement (ici, les prestataires de services). Comme indiqué plus haut, il conviendrait d'éviter les répétitions inutiles des dispositions du RGPD. Le CEPD recommande donc que les paramètres «*autorisent l'utilisateur à sélectionner activement les finalités et les prestataires de services*».

- En l'absence de **paramètres techniques de confidentialité appropriés**, l'octroi et le retrait du consentement dans un environnement électronique extrêmement complexe peut être considérablement compliqué. Le CEPD soutient donc les amendements qui renforcent l'article 10 et **réclament des paramètres de confidentialité par défaut**. En outre, les paramètres de confidentialité devraient véritablement soutenir l'octroi et le retrait d'un consentement **d'une manière aisée, contraignante et opposable à toutes les parties**. Ceci implique que la dernière phrase du considérant 24 de la proposition de la Commission devrait être une disposition matérielle et une exigence légale. En conséquence, il convient de donner aux utilisateurs finaux la possibilité de «*modifier leurs paramètres de confidentialité à tout moment pendant l'utilisation et [de] leur permettre de prévoir des exceptions ou d'établir une liste blanche de certains sites Web ou de préciser les sites Web dont ils acceptent toujours ou n'acceptent jamais les cookies (de tiers)*».

- **Toute limitation des droits prévue par l'article 11 devrait dûment refléter l'importance de la confidentialité des communications, conformément à la jurisprudence constante de la CJUE.** C'est la raison pour laquelle la portée des limitations devrait être plus restreinte que dans le RGPD et des obligations spécifiques devraient être prévues afin de renforcer la transparence des demandes d'accès. Lorsque la portée est limitée aux infractions pénales graves, cette notion devrait être définie plus précisément. Les exigences minimales permettant d'imposer une mesure législative au titre de l'article 23, paragraphe 2, devraient s'appliquer dans tous les cas.

- **Les autorités chargées de la protection des données devraient se voir confier la surveillance de l'application du règlement «vie privée et communications électroniques».** En tant qu'autorités de contrôle chargées de veiller au respect du RGPD, elles sont les mieux placées pour garantir la sécurité juridique et l'application cohérente de ces deux instruments législatifs étroitement liés. De plus, les autorités chargées de la protection des données occuperont une position idéale pour faire appliquer de manière cohérente le règlement «vie privée et communications électroniques» dans toute l'Union grâce au comité européen de la protection des données.

- **La protection contre les communications non sollicitées devrait être efficace.** Le CEPD se réjouit donc des amendements qui prévoient que des systèmes d'appel semi-automatiques ne soient autorisés qu'avec un consentement et il insiste auprès du législateur de l'UE pour que ce dernier s'assure que de tels systèmes sont clairement compris dans la définition du «système de communication et d'appel automatisé». Il se félicite également des amendements qui prévoient des mesures techniques efficaces, en particulier l'application combinée de l'affichage du numéro appelant et de l'utilisation d'un indicatif permettant d'identifier les appels non sollicités, et il est favorable à l'élargissement de l'étendue de la protection à toutes les formes de communications non sollicitées plutôt qu'aux seules «communications de prospection directe».

Les pages suivantes présentent les recommandations du CEPD sur les points essentiels précités.

1. Tout traitement de données de communications doit être fondé sur un motif juridique au titre du règlement «vie privée et communications électroniques» (article 6, considérant 5)

L'un des principaux avantages potentiels du projet de règlement «vie privée et communications électroniques» est le fait que, à l'instar de la directive du même nom aujourd'hui, il apporterait une protection supplémentaire aux communications électroniques en limitant et en précisant les motifs juridiques sur la base desquels ces données peuvent être traitées.

Le CEPD se réjouit des amendements proposés à l'article 6, qui précisent que «**nonobstant l'article 6 du [RGPD]**», les données des communications électroniques **ne peuvent être traitées que** [sur la base des motifs juridiques visés dans le règlement «vie privée et communications électroniques»]. Cet article tel que modifié contribue à assurer la clarté et la sécurité juridique concernant le fait que d'autres motifs juridiques, comme l'intérêt légitime, ne s'appliquent pas au traitement réalisé au titre de la proposition de règlement.

Le CEPD se félicite aussi de l'amendement LIBE 4, lequel clarifie également, en modifiant le cinquième considérant, que le traitement ne devrait être autorisé que «*sur le fondement d'un motif juridique spécifiquement prévu dans le règlement ["vie privée et communications électroniques"]*». À titre d'amélioration supplémentaire, le CEPD recommanderait de reformuler cette phrase pour que cette disposition s'applique à toutes les parties et pas uniquement aux prestataires de services de communications électroniques.

Comme il le préconisait dans son avis, le CEPD est également favorable aux amendements qui préciseraient dans une disposition matérielle que «***ni les fournisseurs de services de communications électroniques ni les tiers ne peuvent traiter des données à caractère personnel collectées sur la base du consentement ou de tout autre motif juridique au titre du règlement "vie privée et communications électroniques»", sur le fondement d'une autre base juridique qui ne serait pas spécifiquement prévue dans le règlement «"vie privée et communications électroniques"».***

2. Les motifs juridiques prévus dans le règlement «vie privée et communications électroniques» ne doivent pas inclure l'intérêt légitime

Certains **amendements proposent une exemption supplémentaire à la confidentialité des communications sur la base de l'intérêt légitime** des prestataires de services et d'autres parties à traiter des données des communications électroniques.

Ni la directive «vie privée et communications électroniques» actuelle ni la proposition de règlement ne contiennent une telle exemption et le projet de rapport n'a pas proposé d'exemption de ce type, pas plus pour les métadonnées que pour le contenu. Les autorités

chargées de la protection des données et des experts indépendants partagent ce point de vue et tous conviennent qu'**une exemption supplémentaire fondée sur l'intérêt légitime, que ce soit pour les métadonnées ou le contenu, risquerait de créer un vide juridique et supprimerait une grande partie de la protection apportée par le règlement «vie privée et communications électroniques» en ce qui concerne la confidentialité des communications.** [3]

Le législateur devrait garder à l'esprit que les informations relatives aux circonstances des communications et aux participants à celles-ci sont expressément protégées par le droit fondamental au secret des communications et que, en tant que tel, il est protégé par la constitution et l'ordre juridique de nombreux États membres. Autoriser le traitement de données liées aux communications sans consentement ou pour une finalité limitée qui est spécifiquement prévue et énoncée avec suffisamment de précision dans la législation pourrait porter atteinte à l'essence même de ce droit fondamental et faire disparaître la tradition des messagers dignes de confiance.

Par ces motifs, le CEPD s'oppose fermement à tout amendement qui introduirait l'intérêt légitime comme fondement d'un traitement au titre du règlement «vie privée et communications électroniques». **Une possibilité de traitement ultérieur ne doit pas ouvrir une porte dérobée réduisant le niveau élevé de protection de la confidentialité des communications.**

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

Le CEPD prend acte des amendements introduits à l'article 7, qui suggèrent que «*l'utilisateur peut en outre, s'il y a lieu, traiter ultérieurement les données conformément aux dispositions du [RGPD]*». Cette clarification est également acceptable, en plus des amendements suggérés plus haut.

Parallèlement, le CEPD s'oppose fermement à tout amendement qui permettrait plus largement les traitements ultérieurs, dans la mesure où ceci porterait gravement atteinte à la protection de la confidentialité des communications et créerait une faille dangereuse permettant de contourner le règlement, comme il l'avait expliqué dans son avis.

3. La confidentialité des données de communications doit être garantie «au repos» et pour les communications de machine à machine (article 5)

Dans l'avis, le CEPD affirmait que le règlement «vie privée et communications électroniques» doit non seulement garantir clairement la confidentialité et la sécurité des communications **en transit**, mais qu'il doit également protéger la confidentialité et la sécurité des équipements des utilisateurs finaux et des données de communications stockées dans le **«nuage». Le CEPD recommandait de revoir l'article 5 et le considérant 15 de la proposition de manière à couvrir clairement ces deux situations.**

À cet effet, le CEPD suggérerait également d'étendre cette disposition pour couvrir les données des communications en transit, mais aussi lorsqu'elles sont stockées par le prestataire de service ou toute autre partie (un exemple typique peut être le contenu de courriels stockés dans le «nuage»). Les amendements à l'article 5 qui précisent que l'interdiction énoncée au paragraphe 1 s'applique également aux «***données des communications électroniques qui sont stockées lorsque leur transmission a été réalisée***» (voir LIBE 399 et 400) sont un bon exemple du type de formulation qui peut être utilisée à cet effet. La formule utilisée dans le LIBE 401 («*que [ces données] soient en transit ou stockées*») peut également être utile.

Comme expliqué dans l'avis du CEPD, **la protection de la confidentialité des communications ne devrait pas dépendre du fait que les personnes parlent ou écoutent, qu'elles écrivent ou lisent le contenu d'une communication, ou qu'elles se fient simplement aux caractéristiques de plus en plus intelligentes de leurs terminaux pour communiquer du contenu en leur nom.**

À cet effet, le CEPD souscrit aux amendements (basés sur les LIBE 59, 409 et 410) qui prévoient que «*la confidentialité des communications électroniques s'applique également aux données **liées** aux équipements terminaux ou **traitées** par ceux-ci*». La même disposition pourrait être formulée comme suit: *«l'interdiction énoncée au paragraphe 1 s'applique également aux données liées aux équipements terminaux ou traitées par ceux-ci»*.

4. Les données liées à l'équipement terminal méritent également un niveau élevé de protection

La protection des données liées à l'équipement terminal devrait être mise en œuvre conformément aux évolutions technologiques et dans le respect du principe de confidentialité des communications et de la règle selon laquelle le règlement «vie privée et communications électroniques» ne devrait pas abaisser le niveau de protection conféré par la directive «vie privée et communications électroniques» actuelle et par le RGPD.

Le CEPD se félicite donc des amendements qui exigent le consentement de l'utilisateur et suppriment l'exception trop générale visée à l'article 8, paragraphe 2, point b), de la proposition de la Commission. Le CEPD est aussi favorable au fait que les informations fournies aux utilisateurs entraînent une exigence supplémentaire de respect du principe de transparence et ne deviennent pas une base juridique pour tracer des personnes physiques dans le temps et l'espace pour n'importe quelle finalité. Il soutient les amendements précisant que lorsque le traitement est autorisé à la seule fin d'établir une connexion, il est limité au temps nécessaire.

Parallèlement, le CEPD n'est pas favorable à l'ajout d'autres motifs juridiques détaillés au règlement «vie privée et communications électroniques» en vue d'instaurer de nouvelles exceptions spécifiques (à l'exception éventuelle très étroite du «comptage des personnes»).

Néanmoins, si de telles exceptions détaillées devaient être proposées dans le cadre d'un compromis à un moment donné de la procédure législative, il convient de garantir à tout le moins qu'elles soient formulées de manière à éviter la création de lacunes involontaires. Outre le «comptage des personnes», ceci s'applique aussi aux motifs juridiques proposés concernant l'établissement d'une connexion, les mises à jour de sécurité, les relations de travail et la mesure d'audience du Web.

- S'agissant du **«comptage des personnes»**, le CEPD recommande à tout le moins d'ajouter des exigences afin de s'assurer que «la finalité du traitement est limitée à un simple décompte statistiques des personnes physiques ou des objets», que «les données sont rendues anonymes dans les plus brefs délais après la collecte», que le traitement est «strictement limité à une zone géographique distincte et délimitée» et que «les utilisateurs disposent de possibilités effectives de ne pas participer».

- S'agissant de **«l'établissement d'une connexion»**, le CEPD est favorable aux amendements qui précisent que ceci doit avoir lieu à la «seule fin» d'établir une connexion «demandée par l'utilisateur».

- S'agissant de la **«mesure de l'audience du Web»**, le CEPD réitère sa préoccupation quant au fait que ce motif doit être défini et interprété de manière étroite et ne devrait pas être indûment élargi durant la procédure législative. Les amendements visant à ajouter l'exigence que «cette mesure ne porte pas atteinte aux droits fondamentaux de l'utilisateur» sont bienvenus.

- S'agissant des **«mises à jour de sécurité»**, le CEPD recommande à tout le moins qu'elles doivent être «strictement nécessaires» et «ne pas réduire le niveau de confidentialité offert par les paramètres de l'utilisateur» et que l'utilisateur soit «informé avant chaque mise à jour» et ait «la possibilité de désactiver l'installation automatique de ces mises à jour».

- S'agissant des **exceptions proposées dans le cadre de l'emploi**, toute exception doit être «strictement limitée à ce qui est nécessaire à l'accomplissement d'une tâche du salarié», «limitée aux cas où l'employeur fournit et/ou est l'abonné de l'équipement terminal» et «l'employeur n'invoque pas ce motif juridique pour contrôler ses salariés».

5. Des définitions appropriées sont indispensables pour mettre en œuvre la protection des droits fondamentaux (article 4)

5.1 Remplacement de la référence aux définitions du code des communications électroniques européen par des définitions indépendantes (article 4)

Pour certaines définitions essentielles[4], la proposition renvoie le lecteur au code des communications électroniques européen (ci-après le «code»).

Comme il le préconisait dans son avis, le CEPD se félicite des amendements qui remplacent la référence au code, toujours en cours de procédure législative, par des définitions indépendantes (voir LIBE 46 et suivants). Il importe de veiller à ce que les définitions utilisées dans le règlement «vie privée et communications électroniques» soient indépendantes de la proposition de code et que les termes essentiels soient définis dans le règlement proprement dit.

Des définitions indépendantes sont particulièrement importantes dans tous les cas où la définition d'un terme diffère, en un ou plusieurs éléments significatifs, de la définition utilisée dans le code, comme la définition du «service de communications interpersonnelles», qui doit également comprendre les «services qui rendent possible une communication interpersonnelle et interactive uniquement en tant que fonction accessoire». Le CEPD se réjouit des amendements qui tendent à apporter ces clarifications.

Des définitions indépendantes sont aussi importantes dans tous les autres cas, même lorsque les définitions du code paraissent actuellement adéquates, étant donné qu'elles peuvent être modifiées dans le cadre de la procédure législative distincte en cours. C'est la raison pour laquelle le CEPD recommande qu'une définition indépendante soit également donnée pour un «appel», au lieu de se référer à l'article 2, paragraphe 21, du code, comme le fait le projet de rapport.

5.2 Définition d'un «utilisateur» et/ou d'un «utilisateur final»

Le CEPD se réjouit des amendements qui visent à réintroduire la définition de l'«utilisateur» en se fondant sur la définition actuelle contenue dans la directive «vie privée et communications électroniques», à savoir: «*toute personne physique utilisant un service de communications électroniques accessible au public à des fins privées ou professionnelles, sans être nécessairement abonnée à ce service*».

Si ces amendements sont adoptés, **il est toutefois également crucial que le terme «utilisateur» soit utilisé de manière cohérente tout au long du règlement en lieu et place de l'expression «utilisateur final»**, qui est définie dans le projet de code et a été utilisée dans la proposition de la Commission.

En règle générale, le terme «utilisateur» devrait être utilisé tout au long du règlement là où il l'était dans la directive actuelle «vie privée et communications électroniques» dans des dispositions équivalentes. Comme expliqué dans l'avis du CEPD, **il doit être clair que ce sont les personnes concernées et touchées plutôt que, par exemple, leurs employeurs ou leurs propriétaires, qui devraient être en mesure de donner un consentement valable au traitement de leurs communications.**

Il conviendrait toutefois d'accorder une attention particulière au fait que, dans certains cas, notamment lorsqu'une disposition vise spécifiquement à protéger les droits des personnes morales qui demandent ou utilisent un service, ou sont abonnées à celui-ci, un autre terme et une autre définition plus appropriés soient utilisés à la place du terme «utilisateur» ou en plus de celui-ci afin de s'assurer que les entités légales restent également protégées. Dans la directive actuelle, le terme «abonné» est généralement utilisé à cet effet.

5.3 Définition des métadonnées

Les amendements proposés montrent que les députés européens sont conscients des risques que pose le traitement des métadonnées pour la confidentialité et la protection des données. En dépit de cette prise de conscience, les amendements suivent toujours l'approche adoptée dans la proposition et **limitent la notion de métadonnées** aux données «*traitées aux fins de la transmission, la distribution ou l'échange de contenu de communications électroniques*» et/ou aux données «*traitées aux fins de la prestation du service*».

Si cette définition recouvre une grande partie des métadonnées, elle n'est pas exhaustive dans la mesure où elle néglige les métadonnées qui ne sont ni requises *aux fins de la transmission, la distribution ou l'échange de contenu de communications électroniques* ni *traitées aux fins de la fourniture du service*. Les données de localisation dans une application de messagerie instantanée en sont un exemple.

Le CEPD propose donc de modifier comme suit la définition afin de couvrir toutes les métadonnées:

c) «métadonnées de communications électroniques» les données traitées dans un réseau de communications électroniques ***qui ne sont pas du «contenu de communications électroniques», ainsi que*** *les données diffusées ou émises par l'équipement terminal qui* **fournissent des informations supplémentaires sur la communication ou servent à identifier l'équipement terminal des utilisateurs finaux dans le réseau ou** *lui permettent de se connecter à ce réseau ou à d'autres équipements terminaux.*

Elles incluent, sans s'y limiter, *les données utilisées pour retracer et déterminer la source et la destination d'une communication, les données relatives à la localisation de l'appareil et la date, l'heure, la durée et le type de communication.*

6. Le consentement doit avoir le même sens que dans le RGPD, notamment être librement donné et spécifique (articles 6, 8 et 9). Les paramètres techniques et de confidentialité devraient véritablement et aisément soutenir l'octroi et le retrait du consentement (articles 9 et 10)

S'agissant de l'article 9, paragraphe 1, le CEPD se félicite des amendements **qui précisent que toutes les dispositions du RGPD relatives au consentement** (y compris l'article 8 du RGPD sur le consentement des enfants) **s'appliquent également aux fins du règlement «vie privée et communications électroniques»**. En particulier, le CEPD est favorable au libellé suivant: «*Les définitions et les conditions du consentement définies par le règlement (UE) 2016/679, notamment, entre autres, son article 4, paragraphe 11, et ses articles 7 et 8, s'appliquent*». Si ce libellé est adopté, les répétitions inutiles des éléments constitutifs du consentement, comme le consentement «spécifique», peuvent être supprimées.

Les éléments du consentement, notamment le consentement librement donné, impliquent que le traitement n'a pas d'effets négatifs sur les droits et libertés de la personne. Le CEPD est donc favorable aux amendements exigeant qu'«***un traitement fondé sur le consentement ne doit pas porter atteinte aux droits et libertés des personnes dont les données à caractère personnel sont liées aux communications ou transmises par celles-ci****, en particulier leurs droits au respect de la vie privée et à la protection des données à caractère personnel*».

Le CEPD soutient fermement les amendements qui renforcent le principe selon lequel le consentement doit être donné librement et qui interdisent les approches du type «à prendre ou à laisser». En particulier, il est favorable aux amendements proposés à l'article 6, qui précisent que le consentement au traitement ne doit pas conditionner «***l'accès au service ou son utilisation***». Ceci devrait s'appliquer tout à la fois au traitement du contenu et des métadonnées.

Le CEPD soutient également les amendements similaires proposés à l'article 8, qui précisent que le consentement ne doit pas «**conditionner l'accès à un service ou son utilisation ou l'utilisation d'un équipement terminal**». Il se réjouit aussi des amendements proposés qui requièrent qu'«***aucun utilisateur ne se voie refuser l'accès à un quelconque service ou à une fonction de la société de l'information, indépendamment du fait que ce service soit payant ou non, au motif que la personne concernée n'a pas donné son consentement conformément à l'article 8, paragraphe 1, point b), à un traitement de données à caractère personnel et/ou à l'utilisation des capacités de stockage de son équipement terminal qui n'est pas nécessaire à la prestation de ce service ou de cette fonction***».

S'agissant de l'article 9, paragraphe 2, **le CEPD est favorable aux amendements selon lesquels les paramètres techniques visés dans ce paragraphe devraient permettre une**

granularité suffisante en termes de finalités et de prestataires, tout en évitant de répéter inutilement les dispositions du RGPD. Plutôt que de continuer d'améliorer les amendements actuels, la disposition peut indiquer que les paramètres doivent «*permettre à l'utilisateur de sélectionner activement les finalités et les prestataires de services*».

Ces amendements devraient en outre préciser que les **paramètres techniques indiquant les préférences de l'utilisateur «*sont contraignants et opposables aux tiers*»**.

Le CEPD soutient également les clarifications supplémentaires précisant que si un utilisateur donne son consentement, cela entraîne la mise à jour des paramètres de confidentialité préétablis. Cette mise à jour devrait toutefois se limiter au traitement demandé par l'utilisateur pour ce service particulier. (Par exemple, un utilisateur peut accepter d'être tracé sur un site Web d'actualités par un réseau publicitaire spécifique. Cependant, ceci ne devrait pas autoriser ledit réseau publicitaire à tracer l'utilisateur sur un autre site Web, à moins que l'utilisateur n'ait également consenti spécifiquement à être tracé lorsqu'il consulte cet autre site.)

Le CEPD soutient donc fermement les amendements qui renforceraient l'article 10 et **imposeraient des paramètres de confidentialité par défaut**. En conséquence, le CEPD recommande que **les logiciels mis sur le marché** qui permettent les communications électroniques «***offrent par défaut des paramètres protégeant la confidentialité afin d'éviter que toute personne autre que l'utilisateur ne stocke des informations sur l'équipement terminal de l'utilisateur et ne traite des informations déjà stockées sur ledit équipement***».

Il est également favorable aux amendements (voir LIBE 639 et 640) **imposant que les exigences relatives à la protection des données par défaut s'appliquent non seulement aux fournisseurs de logiciels, mais aussi aux fournisseurs de matériel**. Ceci inciterait plus directement et plus fortement les fournisseurs d'appareils pour l'Internet des objets à tenir compte de la protection des données par défaut et dès la conception.

Enfin, **le CEPD considère qu'il est essentiel que les utilisateurs puissent aisément donner ou retirer leur consentement à un niveau granulaire, à des fins spécifiques et vis-à-vis de prestataires de services spécifiques à tout moment, pendant ou après l'installation du logiciel**. Ceci devrait comprendre des moyens faciles de mettre à jour leurs paramètres de confidentialité (par exemple, ajouter ou supprimer une ou plusieurs organisations spécifiques de leurs listes blanches et/ou noires personnelles sauvegardées dans leurs paramètres de confidentialité) sans devoir parcourir une série de paramètres et d'options chaque fois qu'ils consultent un site Web différent.

Dans la pratique, ceci pourrait signifier que des personnes qui consultent un site Web et reçoivent une nouvelle demande de consentement pourraient mettre à jour directement leurs paramètres de confidentialité en cliquant sur l'une des options proposées sur le site Web et leur choix serait ensuite enregistré dans leurs paramètres de confidentialité. Si une personne veut retirer son consentement, le retrait devrait également se faire facilement et de la même façon.

La dernière phrase du considérant 24 de la proposition suggère déjà une telle possibilité en prévoyant que «*les navigateurs Web sont encouragés à proposer aux utilisateurs finaux des moyens faciles de modifier leurs paramètres de confidentialité à tout moment en cours d'utilisation et à leur permettre de prévoir des exceptions ou d'établir une liste blanche de certains sites Web ou de préciser les sites Web dont ils acceptent toujours ou n'acceptent jamais les cookies (de tiers)*». **Le CEPD recommande que ce considérant et cet «encouragement» deviennent une disposition matérielle et une exigence légale.** En outre, cette exigence légale devrait s'appliquer non seulement aux navigateurs Web mais également à tout prestataire

relevant du champ d'application de l'article 10. En conséquence, **le CEPD recommande que l'article 10 inclue une exigence selon laquelle «*le matériel et les logiciels mis sur le marché qui permettent les communications électroniques fournissent aux utilisateurs des moyens faciles de modifier leurs paramètres de confidentialité à tout moment en cours d'utilisation*».**

7. Les limitations des droits devraient avoir une portée limitée (article 11)

Dans son avis, le CEPD partageait l'approche adoptée dans la proposition, selon laquelle seuls certains des motifs énumérés à l'article 23, paragraphe 1, du RGPD peuvent être acceptés comme fondements juridiques pour limiter la portée de certains droits et obligations énoncés dans le règlement «vie privée et communications électroniques». Le respect de la confidentialité des communications, tel qu'il est consacré à l'article 7 de la Charte, est essentiel pour l'exercice d'autres droits fondamentaux et joue donc un rôle distinct. Ce rôle est reconnu par les traditions constitutionnelles de nombreux États membres, qui prévoient un droit distinct pour la protection de la confidentialité des communications. Certaines de ces traditions constitutionnelles limitent la possibilité de restreindre ce droit à la seule lutte contre la criminalité grave. Le CEPD est donc favorable aux amendements qui tendent à atténuer l'ingérence avec ce droit et qui limitent les catégories d'intérêts publics à ceux visés à l'article 23, paragraphe 1, points a) à d), du RGPD.

Il découle de la jurisprudence de la CJUE qu'une ingérence avec les droits consacrés par les articles 7 et 8 de la Charte doit répondre à une stricte nécessité. L'exigence de la *stricte nécessité* est de nature horizontale, quel que soit le domaine en cause, comme le secteur répressif ou commercial[5]. Le CEPD soutient les amendements qui font référence à la «*stricte nécessité*» d'une mesure limitant l'exercice des droits visés à l'article 5 du règlement «vie privée et communications électroniques».

Comme indiqué dans son avis, le CEPD soutient également les amendements qui disposent que le droit de l'Union ou le droit des État membres limitant l'exercice de droits devrait à tout le moins comporter un ensemble de dispositions qui contribuent à garantir la sécurité juridique et des garanties minimales. En fait, cette exigence met en œuvre une jurisprudence constante sur les conditions posées à une limitation licite des droits fondamentaux[6]. À titre d'exemple, une législation qui ne prévoit pas la finalité du traitement ou les catégories de données ne résistera pas à un contrôle juridictionnel, dans la mesure où elle est dépourvue de prévisibilité, porte atteinte à la sécurité juridique et où la nécessité de la mesure législative ne peut être démontrée. En conséquence, la référence à l'article 23, paragraphe 2, du RGPD est d'autant plus nécessaire que la législation prévoit une limitation du droit à la confidentialité telle que celle visée à l'article 5 du règlement «vie privée et communications électroniques».

Étant donné la nécessité de disposer de règles claires et précises répondant au critère de nécessité, les amendements qui font référence à la «criminalité grave» devraient définir plus précisément le degré de gravité, cette définition ne pouvant être laissée entièrement aux soins des États membres[7].

Enfin, le CEPD est favorable à la plus grande transparence possible en matière de demandes d'accès. À cet effet et conformément à son avis, il soutient les amendements qui introduisent des obligations de rapport périodique des prestataires aux autorités de contrôle (en plus de l'obligation déjà prévue dans la proposition de fournir des informations à la demande des autorités de contrôle). Il soutient également les amendements imposant aux prestataires l'obligation de publier des informations sur les demandes d'accès.

8. L'affaiblissement de la confidentialité et de l'intégrité des communications devrait être interdit (article 17)

Les limitations des droits visées à l'article 11 peuvent comprendre des mesures techniques destinées à accéder aux données de communications. Dans son avis, le CEPD soutenait le droit des utilisateurs de recourir au cryptage et l'interdiction de toute mesure de décryptage. Il est donc favorable aux amendements interdisant l'affaiblissement général de la confidentialité et de l'intégrité des communications électroniques tant au niveau du service proprement dit qu'au niveau de l'équipement terminal de l'utilisateur (par exemple, en rendant obligatoire l'intégration d'accès dérobés).

Eu égard aux observations qui précèdent, le CEPD est favorable aux amendements basés sur les LIBE 776 à 780.

9. Les autorités chargées de la protection des données devraient disposer de pouvoirs de contrôle (article 18)

Dans son avis, le CEPD soutenait la proposition, qui confiait aux autorités chargées de la protection des données le contrôle de l'application du règlement «vie privée et communications électroniques». Il soutient toujours cette approche, dans la mesure où elle garantit la sécurité juridique et une application cohérente du cadre relatif à la protection des données, par exemple en ce qui concerne l'interprétation de concepts clés comme le «consentement». Cette approche évite également la duplication éventuelle des rôles entre les autorités chargées de la protection des données et d'autres autorités, notamment le chevauchement des compétences, par exemple dans le cas où une autre autorité que celle chargée de la protection des données serait compétente en matière de confidentialité des communications impliquant le traitement de données à caractère personnel. Le CEPD ne souscrit pas aux amendements qui prévoient la représentation de toutes les autorités nationales compétentes (et pas uniquement des autorités chargées de la protection des données) au sein du comité européen de la protection des données. Ces amendements modifieraient considérablement la configuration institutionnelle contenue dans le RGPD et accroîtraient la complexité – en la rendant peut-être ingérable. Les règles actuelles disposent que seules les autorités chargées de la protection des données sont membres du comité européen de la protection des données et, lorsqu'il existe plusieurs autorités chargées de la protection des données, les États membres doivent désigner un représentant commun.

D'autre part, le CEPD est favorable aux amendements qui renforcent la coopération entre les autorités de régulation nationales et les autorités chargées de la protection des données. Ces amendements réclamant une obligation de coopération mutuelle complètent la proposition de la Commission, qui imposait déjà unilatéralement aux autorités chargées de la protection des données de coopérer avec les autorités de régulation nationales.

Enfin, un contrôle efficace ne peut avoir lieu que si des ressources adéquates sont effectivement fournies. Conformément au RGPD, le CEPD doit assurer le secrétariat du comité européen de la protection des données et fournir le personnel nécessaire à cette fin. Le CEPD suggère donc d'inclure une disposition imposant aux États membres et à l'autorité budgétaire de l'Union de fournir des ressources adéquates aux autorités nationales chargées de la protection des données et au CEPD, respectivement.

10. La protection contre les communications non sollicitées devrait être efficace (article 16)

Le CEPD se réjouit des amendements visant à remplacer le mot «*ou*» entre les points a) et b) de l'article 16, paragraphe 3, par «*et*». En effet, ces amendements feront en sorte que la présentation de l'identité d'une ligne sur laquelle la personne physique ou morale qui effectue l'appel peut être contactée [article 16, paragraphe 3, point a)] et l'utilisation d'un code ou d'un indicatif spécifique indiquant qu'il s'agit d'un appel commercial [article 16, paragraphe 3, point b)] ne resteront pas des options alternatives, comme le prévoit la proposition, mais seront toutes deux obligatoires.

Le CEPD est également favorable aux amendements ajoutant le verbe «envoyer» au verbe «présenter», ce qui aligne le libellé actuel sur les développements technologiques.

Le CEPD se félicite des amendements prévoyant que les appels téléphoniques semi-automatiques (c'est-à-dire utilisant des systèmes automatisés pour connecter une personne à l'appelé) soient traités de la même manière que les systèmes entièrement automatisés et requièrent donc un consentement préalable (choix positif). Dans ce cas, des registres nationaux ou européens de numéros exclus pourraient être envisagés pour les appels (purement) vocaux (à l'exclusion des appels semi-automatiques).

Le CEPD est également favorable aux amendements prévoyant que *«l'envoi de messages non sollicités sous une fausse identité, une fausse adresse de réponse ou un faux numéro est interdit»*. Cette interdiction devrait s'appliquer quelle que soit la finalité de la communication non sollicitée (par exemple, une tentative d'hameçonnage peut être tout aussi illicite, voire plus, que des communications de prospection non sollicitées).

Enfin, comme expliqué dans son avis, le CEPD est aussi favorable aux amendements élargissant et clarifiant la définition et la portée des «*communications de prospection directe*» ainsi que ceux protégeant contre toutes formes de «*communications non sollicitées*».

Bruxelles, le 5 octobre 2017

[1] Les présentes observations tiennent compte: (i) du projet de rapport («*projet de rapport*») préparé par le député européen Marju Lauristin pour la commission LIBE; (ii) des (projets d')avis des trois autres commissions parlementaires compétentes (IMCO, IURI et ITRE) et (iii) des amendements supplémentaires 136 à 827 déposés par des membres de la commission LIBE sur le projet de rapport. Tous les documents pertinents du PE sont disponibles sur l'Observatoire législatif du Parlement européen à l'adresse:
http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2017/0003(COD)&l=FR
Le CEPD prend également acte des développements intervenus au Conseil. Voir, par exemple, doc. 11955/17 du Conseil du 8 septembre 2017.

[2] À titre d'exemple, certains amendements portant sur l'article 19 suggèrent une liste de sujets sur lesquels le comité européen de la protection des données devrait publier des orientations. Une référence générale à la possibilité de publier de telles orientations, comme le prévoit déjà la proposition de la Commission, devrait suffire. De même, les voies de recours prévues à l'article 21 pourraient simplement renvoyer aux articles correspondants du RGPD et être complétées par les catégories de personnes ayant accès à ces voies de recours, comme les utilisateurs finaux.

[3] Voir avis 6/2017 du CEPD, avis 1/2017 du groupe de travail «Article 29» et rapports de chercheurs indépendants, comme l'étude commandée par la commission LIBE et préparée en 2017 par Borgesius e.a., disponible à l'adresse:
http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583152/IPOL_STU(2017)583152_EN.pdf

[4] Par exemple, pour la définition d'un «réseau de communications électroniques», d'un «service de communications électroniques», d'un «service de communications interpersonnelles», d'un «service de communications interpersonnelles fondé sur la numérotation», d'un «service de communications interpersonnelles non fondé sur la numérotation», de l'«utilisateur final» et d'un «appel».

[5] Voir également CEPD, *Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel*, II.4, et avis récent de la CJUE 1/15, point 140, qui réaffirme le critère de stricte nécessité.

[6] point 141, qui affirme qu'une mesure limitant l'exercice de droits doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales et indiquer en quelles circonstances et sous quelles conditions une mesure limitant un droit peut être prise.

[7] Avis 1/15 de la CJUE, point 141, en combinaison avec le point 177.