Déclaration du comité européen de la protection des données sur la révision de la directive ePrivacy et son incidence sur la protection de la vie privée et la confidentialité des communications électroniques

Les autorités chargées de la protection des données de l'Union européenne, réunies au sein du comité européen de la protection des données, estiment que la révision de l'actuelle directive ePrivacy (2002/58/CE, modifiée par la directive 2009/136/CE) constitue une étape importante et nécessaire qu'il convient de mener à bien rapidement. L'utilisation des services de communication utilisant le protocole IP s'est fortement répandue depuis 2009, et ces services «par contournement» ne sont actuellement pas couverts par la directive existante. Afin de protéger la confidentialité des communications des utilisateurs finaux lors de l'utilisation de ces nouveaux services et de créer des conditions de concurrence équitables pour les fournisseurs de services de communications électroniques et de services équivalents sur le plan fonctionnel, nous invitons la Commission européenne, le Parlement et le Conseil à collaborer pour garantir une adoption rapide du nouveau règlement ePrivacy, qui remplacera la directive actuelle dès que possible après l'entrée en vigueur du règlement général sur la protection des données (RGPD) en mai de cette année.
Compte tenu de l'évolution des discussions sur la proposition de règlement, le comité européen de la protection des données a décidé de fournir au législateur des conseils et des clarifications sur certaines questions spécifiques soulevées par les amendements qu'ils ont proposés.

1. La confidentialité des communications électroniques nécessite une protection spécifique allant au-delà du RGPD.

La confidentialité des communications (l'équivalent moderne du secret de la correspondance) est un droit fondamental protégé par l'article 7 de la charte des droits fondamentaux de l'Union européenne, déjà mis en œuvre par la directive ePrivacy. Ce droit à la confidentialité s'applique à toutes les communications électroniques, quels que soient les moyens par lesquels elles sont envoyées de l'expéditeur au destinataire et indépendamment du fait que les données soient « au repos » ou « en transit ». Il doit également protéger l'intégrité du terminal de chaque utilisateur.

Les communications électroniques sont indispensables à de nombreuses activités essentielles de nos sociétés modernes, car elles permettent l'exercice de nombreux droits fondamentaux tels que les libertés de pensée, de conscience, de religion, d'expression, d'information, de réunion, d'association, etc. Renforcer la confidentialité et la neutralité des services de messagerie chargés d'acheminer nos communications est donc une nécessité.

Compte tenu de l'importance et de l'utilisation généralisée des communications électroniques dans nos vies numériques, il est fort probable qu'elles contiennent ou révèlent des catégories particulières de données à caractère personnel, soit de manière explicite, soit en raison de l'accumulation et de la combinaison du contenu des communications électroniques ou de leurs

métadonnées, qui peuvent permettre de tirer des conclusions très précises sur la vie privée des personnes, ce qui entraîne des risques élevés pour leurs droits et leurs libertés. Ces communications électroniques devraient donc être traitées en conséquence.

Par conséquent, nous soutenons pleinement l'approche de la proposition de règlement, qui repose sur un principe général d'interdiction, des exceptions limitées, et le recours au consentement. Dès lors, il ne devrait pas être possible, en vertu du futur règlement ePrivacy de traiter le contenu des communications électroniques et leurs métadonnées sur la base de motifs qui ne sont pas délimités clairement, tel que l'«intérêt légitime», et qui vont au-delà de ce qui est nécessaire pour la fourniture d'un service de communications électroniques. En outre, il ne devrait pas être possible de traiter des métadonnées de communications électroniques aux fins de l'exécution d'un contrat ; cela signifie qu'il ne devrait pas y avoir d'exception fondée sur la finalité générale de l'exécution d'un contrat, dès lors que la proposition de règlement, comme la directive ePrivacy actuelle, définissent de façon précise les traitements autorisés à cette fin, telle que celui nécessaire à la facturation.

Le comité européen de la protection des données tient à souligner que les métadonnées de communications électroniques peuvent quand même faire l'objet d'un traitement ultérieur sans consentement après avoir été réellement anonymisées[1]. Il encourage les fournisseurs de services de communications électroniques à recourir à cette possibilité afin de créer des services innovants tout en préservant la vie privée des utilisateurs.

2. La directive ePrivacy est déjà en vigueur.

La confidentialité des communications électroniques est un droit qui existe déjà aujourd'hui. La directive ePrivacy de 2002, modifiée en 2009, a déjà instauré une interdiction générale du traitement du contenu et des métadonnées des communications électroniques. Ces opérations ne sont possibles que:

- si l'utilisateur a donné son consentement préalable ou
- si elles relèvent de l'une des exceptions prévues par la directive (transmission d'une communication électronique, facturation).

Les services de transmission de données utilisés pour la fourniture de services dits de machine à machine (M2M) entrent également dans le champ d'application de la directive actuelle. Les dispositions en question sont maintenues dans la proposition de règlement.
De même, la protection des équipements terminaux est déjà un droit. L'utilisation des capacités de stockage de l'équipement terminal de l'utilisateur est définie d'une manière neutre sur le plan technologique. Par conséquent, non seulement les cookies mais aussi toutes les technologies de suivi sont d'ores et déjà soumis au consentement de l'utilisateur ou relèvent de l'une des exceptions prévues dans la directive «vie privée et communications électroniques».

En outre, la proposition de Règlement telle que modifiée par le législateur introduit plusieurs nouvelles exceptions qui ont été proposées par le groupe de travail «article 29»[2], telles que les mises à jour de sécurité et la mesure d'audience. Ces exceptions sont liées à des catégories de traitement spécifiques qui présentent des risques très limités pour la vie privée des utilisateurs.

3. La proposition de Règlement vise à garantir son application uniforme dans tous les États membres et quel que soit le responsable du traitement.

---

[1] Voir à cet égard la définition figurant dans le document WP 216, alors que les données pseudonymisées restent des données à caractère personnel.
[2] Voir WP 194 et WP 240.

L'actuelle directive ePrivacy ne s'applique pas aux services de communications électroniques proposés par des fournisseurs exerçant leurs activités via Internet, alors que ceux-ci proposent un service qui est équivalent sur le plan fonctionnel.
Ces fournisseurs relèveront toutefois du champ d'application de la proposition de règlement. Le comité européen de la protection des données souligne que l'extension du champ d'application du futur règlement aux services équivalents sur le plan fonctionnel, y compris aux services de communication «par contournement», est un élément essentiel de la réforme. Il convient d'éviter toute proposition de modification du futur règlement qui pourrait porter atteinte à cet objectif (par exemple, toute proposition visant à limiter le champ d'application de la protection aux communications «en transit»), afin de garantir des conditions de concurrence égales pour tous les fournisseurs.
La proposition de règlement s'applique également au recueil de données relatives au comportement des utilisateurs, indépendamment du fait que ces derniers aient créé un compte pour un service ou non. Cette approche permettra non seulement aux utilisateurs de ces services de bénéficier de la protection qui leur est due, mais garantira également une concurrence loyale entre les responsables du traitement. Il convient de noter que le consentement qui doit être obtenu en vertu de la proposition de règlement ePrivacy a la même définition que dans le RGPD. En particulier, la nécessité d'obtenir le consentement libre des utilisateurs empêchera les fournisseurs de services de mettre en place des *«cookie wall»*[3], c'est à dire de priver d'accès à leur site les utilisateurs n'acceptant pas les cookies et autres traceurs ; l'obligation d'obtenir le consentement spécifique de ces derniers créera des conditions de concurrence uniformes et équitables pour les fournisseurs, que l'utilisateur soit connecté ou non.
En outre, l'instauration de sanctions spécifiques pour les infractions à la règlementation ePrivacy, combinée à un champ d'application territorial étendu, qui reflètent tous les deux les dispositions du RGPD, conféreront un pouvoir effectif aux autorités de protection des données, ce qui leur permettra de faire appliquer le futur Règlement à tous les outils de communications électroniques utilisés par les citoyens de l'UE.

4. Le nouveau règlement doit imposer l'obligation de recueil du consentement pour les cookies et les technologies similaires et offrir aux fournisseurs de services des outils techniques leur permettant d'obtenir ce consentement.

Tel que formulé par la Commission européenne, l'article 10 de la proposition de règlement vise à permettre aux utilisateurs d'exercer un contrôle sur l'utilisation des capacités de stockage de leurs équipements terminaux. Cet article a été remanié par le Parlement pour exiger la prise en compte du principe de la protection de la vie privée par défaut dans les paramètres des logiciels et pour fournir une solution technique permettant aux sites web d'obtenir un consentement valable.
Le comité européen de la protection des données soutient sans réserve le renforcement de cet article et considère qu'il devrait s'appliquer explicitement aux systèmes d'exploitation des téléphones intelligents, des tablettes et aux autres «agents utilisateurs», afin de garantir que les applications de communication prennent en compte les choix de leurs utilisateurs, quels que soient les moyens techniques utilisés.
Par ailleurs, les paramètres de confidentialité devraient permettre à l'utilisateur de donner et de retirer son consentement de manière aisée, contraignante et exécutoire à l'égard de toutes les parties, et il devrait se voir proposer un choix clair lors de l'installation, lui permettant de donner son consentement s'il le souhaite. En outre, les sites web et les applications mobiles devraient pouvoir recueillir le consentement d'un utilisateur conformément au RGPD au moyen des réglages de protection de la vie privée.

[3] Un «*cookie wall*» empêche les utilisateurs qui ne donnent pas leur consentement d'accéder à un site ou à un service internet.

5. Conclusions

Le comité européen de la protection des données considère que:

- Le futur règlement ePrivacy ne devrait pas baisser le niveau de protection offert par l'actuelle directive ePrivacy.
- Le futur règlement ePrivacy devrait, d'une manière neutre sur le plan technologique, garantir la protection de tous les types de communications électroniques, y compris de celles effectuées au moyen de services « par contournement ».
- Le consentement de l'utilisateur devrait être obtenu systématiquement d'une manière techniquement viable et exécutoire avant tout traitement des données de communications électroniques et avant toute utilisation des capacités de stockage ou de traitement des équipements terminaux d'un utilisateur. Il ne devrait y avoir aucune exception pour le traitement de ces données sur la base de l'«intérêt légitime» du responsable du traitement ou de l'exécution d'un contrat de façon générale.
- L'article 10 devrait fournir un moyen efficace d'obtenir le consentement des utilisateurs pour les sites web et les applications mobiles. D'une manière plus générale, les paramètres devraient protéger la vie privée des utilisateurs par défaut, et ces derniers devraient être guidés dans le choix d'un paramètre, sur la base d'informations pertinentes et transparentes. À cet égard, le futur règlement devrait rester neutre sur le plan technologique afin de veiller à ce que son application soit cohérente, quels que soient les cas d'usage.
- Toute exception ad hoc que les législateurs envisageraient d'ajouter à celles déjà prévues dans les projets de la Commission et du Parlement devrait faire l'objet d'un examen rigoureux. En particulier, toute exception définie dans des termes larges pour les cas où une «autorité publique» souhaiterait procéder au traitement de données de communication devrait être soigneusement examinée et la proposition ne devrait pas permettre un suivi systématique de la localisation des utilisateurs ni le traitement des métadonnées de leur communications électroniques.
- Pour que le consentement puisse être librement accordé conformément au RGPD, l'accès aux services et aux fonctionnalités ne doit pas être subordonné au consentement de l'utilisateur au traitement de ses données à caractère personnel ou d'informations relatives à son équipement terminal ou traitées par celui-ci. En d'autres termes, les « cookies walls » devraient être explicitement interdits.
- Il convient d'encourager l'utilisation de données de communications électroniques réellement anonymisées.
- Les évolutions susmentionnées permettront de protéger la vie privée des utilisateurs finaux dans tous les contextes pertinents et de prévenir toute distorsion de la concurrence.