CNEJITA, le 19 juin 2018

La proposition de règlement « vie privée et communications électroniques » (règlement E-Privacy)

Isabelle GAVANON

Directeur Associé – Fidal

Membre du Conseil d'administration de l'AFDIT

Introduction

Plan

1. Champ d'application du projet de règlement e-Privacy
2. L'article 5, confidentialité des données
3. L'article 6, traitement licite des données de communications électroniques
4. L'article 7, stockage et effacement des données
5. L'article 8, protection des informations
6. L'article 9, consentement
7. L'article 10, informations à fournir et options à proposer pour les paramètres de confidentialité
8. L'article 16, communications non sollicitées
9. L'article 17, risques de sécurités détectées

1. Champ d’application du projet de règlement e-Privacy

1. Champ d'application du projet de règlement e-Privacy

1.1 Les acteurs

1.2 Les données

1.3 Les bénéficiaires

1.1 Les acteurs

1.1 Les acteurs

- les opérateurs et télécoms traditionnels

- les « nouveaux » fournisseurs de services de communications électroniques dit fournisseurs de services de contournement (OTT) : VoIP, Messagerie instantanée (WhatsApp, skype), courrier électronique web,

1.1 Les acteurs

Sont également concernés :

- les objets connectés et la communication entre machines
- les fournisseurs d'annuaires accessibles au public et
- les fournisseurs de logiciels permettant des communications électroniques, y compris la récupération et la présentation d'informations sur Internet,
- les personnes physiques et morales utilisant des services de communications électroniques pour envoyer des communications commerciales de prospection directe ou recueillir des informations qui concernent l'équipement terminal de l'utilisateur final ou qui y sont stockées

1.2 Les données

1.2 Les données

Les données prises en compte par ce règlement sont les données de communication :

- le contenu de communications électroniques,
- les métadonnées de communications électroniques.

1.2 Les données

L'article 3.l du projet de la Commission, défini le contenu de communications électroniques comme étant :

« le contenu échangé au moyen de services de communications électroniques, notamment sous forme de texte, de voix, de documents vidéo, d'images et de son »

De plus son article 4.3.m défini les métadonnées comme étant :

« les données traitées dans un réseau de communications électroniques aux fins de la transmission, la distribution ou l'échange de contenu de communications électroniques, y compris les données permettant de retracer une communication et d'en déterminer l'origine et la destination ainsi que les données relatives à la localisation de l'appareil produites dans le cadre de la fourniture de services de communications électroniques, et la date, l'heure, la durée et le type de communication »

1.2 Les données

Mais aussi :

- les adresses IP, logs de connexion, géolocalisation,… qui permettent de tirer des conclusions précises sur la vie privée des personnes intervenant dans la communication électronique, comme leurs rapports sociaux, leurs habitudes et activités au quotidien, leurs intérêts, leurs goûts, etc,

- les informations liées aux équipements terminaux des utilisateurs.

1.2 Les données

Exemple d'utilisation commerciale de métadonnées :

La fourniture de cartes de densité de clics, représentation graphique de données à l'aide de couleurs pour indiquer la présence d'individus, pour afficher les mouvements de trafic dans certaines directions au cours d'une période de temps déterminée, un identificateur est nécessaire pour relier les positions des individus à des intervalles de temps donnés.

Une telle utilisation des métadonnées de communications électroniques pourrait, par exemple, permettre aux pouvoirs publics et aux exploitants de transports publics de déterminer où développer de nouvelles infrastructures en fonction de l'usage des structures existantes et de la pression que celles-ci subissent.

1.3 Les bénéficiaires

1.3 Les bénéficiaires du projet de règlement e-Privacy

- les personnes physiques
- les personnes morales (avec une protection notamment à propos du secret des affaires)

2. L’article 5, confidentialité des données

2. L’article 5, confidentialité des données

Projet de la Commission :

« Les données de communications électroniques sont confidentielles. Toute interférence avec des données de communications électroniques, comme l'écoute, l'enregistrement, le stockage, la surveillance et d'autres types d'interception, de surveillance ou de traitement des données de communications électroniques, par des personnes autres que l'utilisateur final est interdite, sauf dans les cas où le présent règlement l'autorise. »

2. L’article 5, confidentialité des données

Projet du Parlement européen :

La confidentialité des communications électroniques s’applique également aux données liées aux équipements terminaux et à celles traitées par ceux-ci.

La fédération du marketing direct s’opposait à cet ajout.

3. L’article 6, traitement licite des données de communications électroniques

3. L'article 6, traitement licite des données de communications électroniques

Projet de la Commission :

1. Les fournisseurs de réseaux et de services de communications peuvent traiter les **données** de communications électroniques :

- pour assurer la communication pendant la durée nécessaires à cette fin ;
- maintenir ou rétablir la sécurité des réseaux et services ou détecter des dysfonctionnements pendant la durée nécessaire à cette fin.

Projet du Parlement européen :

Nécessité technique :

- pour maintenir la sécurité du réseau ou service de communications électroniques ;
- pour détecter des défaillances ou erreurs ;
- si strictement nécessaire en matière de qualité, et pour établir les factures.

3. L'article 6, traitement licite des données de communications électroniques

2. Les fournisseurs de services de communications électroniques peuvent traiter les **métadonnées** de communications électroniques pour :

- satisfaire des obligations en matière de qualité de service,
- établir des factures, calculer des paiements,
- éviter la fraude à l'usage et à l'abonnement, ou
- avec le consentement de l'utilisateur final, pour un ou plusieurs objectifs précis, la fourniture de services spécifiques, si le traitement d'informations anonymisées est insuffisant.

Projet du Parlement européen : lorsque le traitement est légal par l'obtention du consentement de l'utilisateur final, un PIA doit être envisagé conformément aux articles 35 et 36 du RGPD.

3. L'article 6, traitement licite des données de communications électroniques

3. Les fournisseurs des services de communications électroniques peuvent traiter **le contenu** de communications électroniques uniquement avec le :

- consentement d'une personne concernée pour un service spécifique qui requiert le traitement des DP

- consentement de toutes les personnes concernées lorsque le traitement anonymisé n'est pas possible : étude d'impacts et consultation de la CNIL

Le principe de minimisation des données, ainsi que des analyses d'impacts, est réaffirmé.

Le Parlement a limité les cas de recours à cette possibilité d'accès

3. L’article 7, stockage et effacement des données

3. L'article 7, stockage et effacement des données

Projet de la Commission :

Le fournisseur de services de communications électroniques efface ou anonymise les données de communications électroniques (contenus et métadonnées) sauf si la conservation est autorisée pour un traitement permis par l'article 6.

Après réception du contenu des communications par l'utilisateur final, le RGPD s'applique

Projet du Parlement européen :

Notamment, il évoque l'effacement quand la donnée concernée n'est plus nécessaire, mais pas l'anonymisation

4. L’article 8, protection des informations stockées dans les équipements terminaux des utilisateurs finaux ou liées à ces équipements

4. L’article 8, protection des informations

Projet de la Commission :

8.1 Utilisation des capacités de traitement et de stockage,

Interdite, sauf si :

- elles sont nécessaires pour assurer une communication électronique ;
- l’utilisateur final a donné son consentement ;
- elles sont nécessaires pour fournir un service demandé par l’utilisateur final ;
- elles sont nécessaires pour mesurer l’audience effectuée par le fournisseur du service.

4. L'article 8, protection des informations

Parlement européen:

Utilisation est possible :

- si elle est **strictement** nécessaire pour assurer une communication électronique ;
- si l'utilisateur donne son consentement **spécifique** ;
- si strictement nécessaire techniquement pour fournir un service demandé par l'utilisateur ;
- si elle est **strictement** nécessaire sur le plan technique pour la mesure d'audience et rajoute la possibilité que la mesure d'audience soit faite par le fournisseur du service ou en son nom ou par une agence indépendante d'analyse pour l'intérêt public ou fins scientifiques
- si elle est nécessaire dans le contexte des relations de travail, sous réserve qu'aucune surveillance du salarié n'en résulte.

4. L’article 8, protection des informations

8.2 collecte d’informations émises par les équipements (Wifi-tracking)

Commission :

Elle est possible :

- à des fins de connexion ;
- pour d’autres finalités, mais les personnes concernées doivent être informées du traitement et des moyens dont elles disposent pour s’y opposer.

Parlement européen :

Il est nécessaire d’obtenir le consentement des personnes ou mettre en place des mesures techniques et juridiques afin de réduire les risques pour les personnes

5. L’article 9, consentement

5. L'article 9, consentement

La définition et les conditions du consentement du RGPD s'appliquent.

La Commission propose de remplacer les bandeaux par un consentement (opt-in) sous forme de paramétrage du navigateur (Il peut être exprimé à l'aide des **paramètres techniques appropriés**.

Le Parlement précise que les paramètres devraient envoyer des signaux aux autres parties les informant des paramètres de confidentialité de l'utilisateur et précise que ces paramètres devraient être contraignants pour tout tiers et lui être opposables.

La Commission : quand l'utilisateur donne son consentement, il a la possibilité de le retirer à tout moment, et cette possibilité doit être rappelée tous les six mois, tant que le traitement se poursuit.

Le Parlement intègre la possibilité de retirer son consentement dans l'article 9.

6. L’article 10, informations à fournir et options à proposer pour les paramètres de confidentialité

6. L’article 10, informations à fournir et options à proposer pour les paramètres de confidentialité

Commission : Les logiciels permettant d’effectuer des communications électroniques (navigateurs ou applications de communication) doivent offrir la possibilité d’empêcher les tiers de stocker des informations sur l’équipement terminal d’un utilisateur final ou de traiter des informations déjà stockées sur ce terminal.

Au moment de l’installation, il convient d’informer l’utilisateur final des paramètres de confidentialité disponibles et avant de continuer l’installation, lui imposer d’en accepter un.

6. L'article 10, informations à fournir et options à proposer pour les paramètres de confidentialité

Parlement : Ces logiciels devront être paramétrés par défaut et dès leurs installation, de manière à ce que le traçage de l'utilisateur et le stockage d'informations sur son terminal soient interdits (Do not track).

Durant l'utilisation du navigateur ou du logiciel, les paramètres qui s'offrent à l'utilisateur devront être facilement accessible pour qu'il puisse les modifier à tout moment, exprimer un consentement spécifique même après installation.

L'utilisateur doit prendre une décision informée et les informations ne doivent pas avoir pour effet de le dissuader de sélectionner des paramètres de confidentialité plus élevées que ceux prévus par défaut.

7. L’article 16, communications non sollicitées

7. L’article 16, communications non sollicitées

Commission :

La prospection directe des personnes physique requiert son consentement (opt-in)

Les partisans d’un usage plus large des données souhaitent le recours à l’intérêt légitime du responsable de traitement et non exclusivement au consentement

Opt out s’il y a fourniture préalable de biens ou services analogues auprès des personnes.

Cela prend en compte la promotion des partis politiques et des organisations à but non lucratif.

7. L’article 16, communications non sollicitées

Parlement européen :

L’utilisation par des personnes de services de communications électroniques, comme systèmes automatisés d’appel, télécopies, courriels ou utilisation autre de services de communications électroniques pour l’envoi de communication de prospection directe aux utilisateurs n’est autorisée que pour les utilisateurs ayant donné un consentement préalable.

De plus, il y a une interdiction de masquer son identité ou d’utiliser de fausses identités ou de fausses adresses de réponse ou de faux numéros lors de l’envoi de communications de prospection directe non sollicitées.

8. L’article 17, risques de sécurités détectées

Le Parlement renforce la proposition de la Commission en termes de sécurité des données de communications et d’information aux abonnés

Conclusion

Contact

Isabelle GAVANON

Avocat– Directeur Associé

Propriété intellectuelle - Technologies de l'information – Contrats

01 47 38 91 06

isabelle.gavanon@fidal.com