RÈGLEMENT E-PRIVACY

UNE PROTECTION ÉLARGIE AUX DONNÉES DE COMMUNICATIONS ÉLECTRONIQUES

Rosa Barcelo

Directrice
du département
Digital Privacy

DG Connect
Commission européenne

INTERVIEW

La Commission européenne a publié en janvier 2017 un projet de règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques (qui abroge la directive Vie privée et Communications électroniques de 2002). Ce règlement complète les dispositions du RGPD et s'intéresse plus particulièrement à la protection des communications électroniques (courriers, SMS, appels vocaux) et à l'utilisation des cookies. Encore à l'état de projet, il devrait pourtant entrer en vigueur, comme le RGPD, en mai 2018.

■ Comment s'articule la proposition de règlement dit « *e-Privacy* »[1] avec le règlement général sur la protection des données personnelles (RGPD)[2] ?

Tout d'abord, le projet de règlement de la Commission et du Parlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques a été élaboré en collaboration avec nos collègues du département Justice qui ont travaillé sur le texte du GDPR afin d'harmoniser les deux textes. L'objectif n'était pas de faire un règlement RGPD bis, mais d'encadrer précisément les enjeux liés aux communications électroniques. C'est-à-dire que le RGPD fournit un cadre général à la protection des données et le règlement *e-Privacy* constitue une « *lex specialis* » par rapport au RGPD. Ainsi, le règlement de la Commission précise et complète le RGPD avec des obligations spécifiques qui s'appliquent aux données de communications électroniques qui peuvent être considérées comme des données à caractère personnel. Toutes les matières relatives au traitement de ces données, qui ne sont pas spécifiquement couvertes par la proposition, le sont par le RGPD comme par exemple les obligations en matière de sécurité ou encore la notification obligatoire à l'utilisateur en cas de perte de ses données. En outre, la proposition de règlement vise aussi à protéger le droit du respect des

[1] Règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement «vie privée et communications électroniques»)

[2] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

communications, tel qu'il est consacré à l'article 7 de la Charte des droits fondamentaux de l'Union européenne.

■ **Est-ce à dire que le réglement *e-Privacy* est plus adapté aux modes de communications électroniques actuels ?**
En effet, avec l'avènement des nouveaux canaux de communications qui ne passent plus directement par les opérateurs de télécom classiques, réformer la directive vie privée et communications électroniques de 2002 en profondeur est devenu nécessaire. Ainsi le projet de règlement *e-Privacy* élargit le périmètre de la protection des données de communication électroniques en faisant rentrer dans son champ d'application les acteurs OTT (*Over the top*), c'est-à-dire des acteurs comme Facebook Messenger, WhatsApp, Viber ou Skype qui offrent tous des nouveaux services de messagerie. Par ailleurs, comme la directive actuelle, le règlement s'appliquera aussi aux échanges entre personnes morales. Par exemple, dans le cadre du commerce en ligne, les opérateurs de télécommunications seront désormais tenus d'une obligation de confidentialité lorsqu'elles transmettront des informations échangées entre personnes morales, même si les données transmises ne sont pas personnelles.

■ **Quel sera l'impact sur les modèles économiques en place, sachant que les éditeurs sont vent debout contre le projet ?**
En partant de la philosophie du texte, il faut savoir que nous avons considéré que l'ordinateur (ainsi que le *smartphone* ou la tablette) appartient à la sphère privée, car il peut contenir des informations sensibles. Or certains *cookies* peuvent également recueillir des données de navigation et tracer les internautes lorsqu'ils visitent un site ou utilisent une application. Un consentement préalable de l'utilisateur est donc nécessaire à l'insertion de traceurs, ne serait-ce que pour éviter que les virus s'emparent de sa machine (ou éviter d'être suivi lorsque l'on utilise Internet). Un paramétrage d'origine ainsi qu'une obligation, au moment de l'installation du logiciel de navigation, d'informer l'utilisateur final des paramètres de confidentialité disponibles, avant de continuer l'installation, évite à l'utilisateur un processus de consentement fastidieux. Cette disposition est à l'image de l'utilisation accrue des logiciels de blocage des *cookies* et autres *spywares* (logiciels espions) par les consommateurs. Cependant, il reste possible aux utilisateurs finaux de donner leur autorisation au cas par cas. Par exemple, le navigateur pourrait établir pour l'utilisateur final une liste de certains sites web dont il accepte les *cookies* espions. L'utilisateur devrait disposer d'un éventail de réglages de confidentialité, depuis les plus restrictifs (« *ne jamais accepter les* cookies ») jusqu'aux plus permissifs (« *toujours accepter les* cookies »), en passant par des options intermédiaires (« *rejeter les* cookies *de tiers* » ou « *accepter uniquement les* cookies *propres* », par exemple). Ces paramètres de confidentialité devraient se présenter sous une forme facile à visualiser et à comprendre. De la même façon, les éditeurs conserveront la liberté d'accorder ou non l'accès au contenu de leurs sites en cas de refus de consentement aux *pop-up* ou *cookies* de leurs plates-formes *web*. Le règlement vise à apporter un équilibre entre les intérêts divers des parties prenantes.
Le projet de règlement *e-Privacy*, y compris l'obligation de consentement, s'applique uniformément à tous les acteurs. Il n'impose pas de modèle économique particulier, que ce soit avec ou sans *login*, et il ne distingue

« L'objectif de la Commission n'est pas de faire un règlement RGPD bis, mais de préciser et compléter le RGPD avec des obligations spécifiques qui s'appliquent aux données de communications électroniques. »

pas entre grands ou petits fournisseurs, car le risque pour la vie prive existe indépendamment de la qualité de l'opérateur qui insère des traceurs.

■ **S'agissant du consentement de l'utilisateur, pouvez vous préciser cette disposition (18) du projet de règlement : « *Le consentement relatif au traitement de données résultant de l'utilisation d'Internet ou des communications vocales ne sera pas valable si la personne concernée ne dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice* ». Que recouvre la notion de « la liberté de choix » dans ce cas ?**
Nous sommes favorables à une liberté totale de choix de donner ou non son consentement sans se trouver pénalisé. La proposition de règlement *e-Privacy* ne contient pas une définition de consentement. Cela comprend la définition du consentement en vertu du règlement (UE) 2016/679 de protection de données personnelles. C'est cette définition qui devrait s'appliquer. Il faudrait voir, au cas par cas, si l'utilisateur final a exprimé ou pas un consentement valable. Il reste évident que les pages qui permettent à l'utilisateur d'accomplir une formalité réglementaire (comme par exemple la déclaration d'impôt en ligne) ne pourront pas être bloquées pour défaut de consentement aux *cookies*.

■ **Quels sont les points susceptibles de susciter des débats que vous appréhendez lors de la présentation du projet de rapport qui aura lieu à l'assemblée, avant un vote en plénière courant octobre ?**
Nous pensons que la proposition est très équilibrée : en étendant son champ d'application à l'ensemble des fournisseurs de services de communications électroniques, le réglement va renforcer le respect de la vie privée dans ces échanges. En même temps, il va créer de nouvelles possibilités de traiter des données de communication et renforcer la confiance et la sécurité dans le marché unique numérique, l'un des objectifs clés de la stratégie de ce marché. Il est difficile de prévoir les points susceptibles de susciter des débats au sein du Parlement européen. Les projets de rapport et des opinions soulèvent différents points, y compris le niveau du paramétrage des logiciels de navigation. Par exemple, on voit que le rapport de Madame Lauristin[3] préconise que les logiciels qui permettent d'effectuer des communications électroniques offrent par défaut 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 ledit terminal.

> *« e-Privacy devrait s'appliquer en même temps que le RGPD afin d'assurer aux consommateurs de l'UE une protection élargie de leurs données personnelles à date, communications électroniques comprises. »*

■ **L'entrée en vigueur du règlement est prévue pour le 25 mai 2018, comme le GDPR, mais eu égard aux oppositions des entreprises du digital qu'il subit, cette date pourra-t-elle être tenue ?**
Oui, la date d'entrée en vigueur le 25 mai 2018 est maintenue et nous œuvrons en ce sens. e-Privacy devrait s'appliquer en même temps que le RGPD afin d'assurer aux consommateurs de l'UE une protection élargie de leurs données personnelles à date, communications électroniques comprises.

■ **Quelle mise en garde pourriez-vous adresser à l'industrie financière très friande des nouvelles technologies d'identification qui recueillent des données des clients sur la toile dans le but « avoué » de se mettre en conformité avec leurs exigences réglementaires (LCB-FT) ?**
Le règlement vie privée s'applique surtout aux fournisseurs de télécom, y compris les OTT. Il y a peu d'articles du règlement qui sont d'application aux opérateurs qui ne sont pas compagnies de télécom. C'est le cas des articles concernant les envois des communications non sollicitées à fin de prospection directe (spam). C'est aussi le cas des *cookies* : obtenir un consentement au stockage des *cookies* est obligatoire. Vis-à-vis de ces articles, les points importants à retenir concernent ceux qui visent à donner aux utilisateurs l'information nécessaire pour qu'ils puissent faire un choix. La transparence reste primordiale. ■

Propos recueillis par Samorya Wilson.

[3] La rapporteure désignée par le Parlement en charge de rédiger une proposition de règlement est l'Estonienne social-démocrate Marju Lauristin. Elle a élaboré un rapport sur le projet *e-Privacy*.