FEDIL

Positionen - 20/08/2017

AVIS DE LA FEDIL – EPRIVACY

Zusammenfassung / Inhalte

COMMENTAIRES GÉNÉRAUX

COMMENTAIRES SPÉCIFIQUES

1. Extension du champ d'application (article 4 (1))
2. Rationalisation et simplification des règles en termes d'utilisation des cookies
3. Annuaires accessibles au public
4. Protection contre les spams et les actes de phishing
5. Consentement

Position qui constitue l'avis des membres FEDIL-ICT relatif à la «proposition de 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»)» publiée par le 10 janvier 2017.

COMMENTAIRES GÉNÉRAUX

FEDIL-ICT accueille favorablement la proposition de la Commission européenne quant à la révision de la directive «vie privée et communications électroniques» (2002/58/CE) qui vise, entre autres, à garantir un niveau élevé de protection de la vie privée aux utilisateurs de services de communications électroniques mais également la confidentialité des informations échangées par voie électronique et ainsi renforcer la confiance des consommateurs dans ces services au niveau européen afin de promouvoir le développement d'un véritable marché intérieur des communications électroniques dans l'Union et ainsi renforcer la compétitivité européenne.

Nous comprenons également l'objectif de la Commission de compléter le Règlement général sur la protection des données (RGPD) par de nouvelles dispositions relatives aux communications électroniques qui ne sont pas couvertes par ce dernier. Il nous semble, en effet, nécessaire de préciser les droits et les obligations des fournisseurs de réseaux et de services de

communications électroniques notamment quant au traitement des données, des métadonnées et des contenus dérivés des communications électroniques.

De plus, nous soutenons fermement la nature *lex specialis* de la proposition et sa cohérence avec le RGPD, ainsi que l'entrée en vigueur, à la même date, des deux règlementations, cela va considérablement faciliter la transition vers le nouveau cadre en matière de protection des données pour les entreprises dans le domaine des communications électroniques. Une telle proposition d'échéancier devrait éviter tout recoupement et incohérence entre le RGPD et l'actuel régime ePrivacy.

COMMENTAIRES SPÉCIFIQUES

1. EXTENSION DU CHAMP D'APPLICATION (ARTICLE 4 (1))

L'utilisation par les consommateurs et les entreprises des nouveaux services Internet permettant des communications interpersonnelles telles que la voix sur IP, la messagerie instantanée et les services de courrier électronique basés sur le Web au lieu des services de communication traditionnels se démocratise alors qu'ils ne sont, en général, pas assujettis au cadre réglementaire actuel de l'Union européenne en matière de communications électroniques. Dès lors, il est nécessaire de soumettre ces services de communication par contournement («OTT») à une réglementation harmonisée au niveau européen afin de renforcer la confiance des consommateurs dans ces services. En conséquence, nous supportons la proposition de la Commission d'étendre le champ d'application de du règlement ePrivacy en mettant en place un certain nombre de dispositions et d'obligations qui s'adressent aux «OTT» afin d'instaurer des conditions de concurrence équitables (level playing field) pour tous les acteurs économiques proposant des services de communications électroniques équivalents. Cela permettra, par ailleurs, d'apporter une sécurité juridique quant à la qualification des infractions commises via ces supports de communications électroniques qui n'étaient jusqu'alors pas soumis aux moyens d'enquêtes notamment.

Néanmoins, nous remettons en question l'utilisation des définitions de l'article 2 points 1), 4), 5), 6), 7), 14), et 21) de la «Proposition de directive établissant le code des communications électroniques européen» dans l'article 4 (1) b. En effet, cette proposition a été adoptée par la Commission européenne le 14 septembre 2016 et se trouve actuellement en processus législatif au sein de la Commission Industrie, recherche et énergie du Parlement européen. Ce texte n'ayant donc pas été voté et de nombreuses propositions d'amendements ayant été déposées, il est, dès lors, fort probable que les définitions soient révisées. C'est pourquoi, nous demandons à la Commission de revoir le texte et de proposer des définitions propres au règlement ePrivacy.

2. RATIONALISATION ET SIMPLIFICATION DES RÈGLES EN TERMES D'UTILISATION DES COOKIES

FEDIL-ICT souhaite ici soulever la question de l'obtention du consentement dans le cas de l'acceptation des cookies tiers tel que cela est stipulé dans l'article 8 (1) b. L'article 9 (2) précise simplement «*si cela est techniquement possible et réalisable, aux fins de l'article 8, paragraphe 1, le consentement peut être exprimé à l'aide des paramètres techniques appropriés d'une application logicielle permettant d'accéder à Internet.*». Cette formulation proposée par la

Commission nous parait relativement floue et ne résout pas les questions, d'une part, du moyen d'obtenir le consentement et d'autre part, des possibilités de traçabilité de ce consentement.

En effet, pour être conforme au RGPD, le responsable du traitement doit être en mesure de prouver l'obtention d'un consentement «libre, spécifique, éclairé et univoque» (article 4 (11) du RGPD). Or, lors de l'installation des cookies tiers et des paramètres de confidentialité, le responsable du traitement ne reçoit aucune information en provenance, par exemple, du moteur de recherche ou du site internet, sur les cookies qui ont été acceptés ou non. Comment peut-il alors prouver que le consentement a été donné pour la fourniture de l'un ou l'autre service? Il nous parait légitime de demander à la Commission de proposer des lignes directrices afin de préciser les moyens techniques à mettre en œuvre pour assurer la traçabilité du consentement permettant ainsi au responsable du traitement de remplir ses obligations légales et réglementaires.

De plus, lors de l'installation des cookies tiers et des paramètres de confidentialité, l'exigence du consentement offre aux utilisateurs finaux l'option de rejeter tous les cookies tiers alors qu'aucun consentement n'est requis pour les cookies propriétaires qui n'entravent pas la vie privée. En effet, la proposition de règlement indique dans l'article 10 (1) et (2) que les logiciels offrent l'option de rejeter tous les cookies tiers. Si une part importante d'utilisateurs finaux opte pour rejeter ces cookies tiers, les petites et moyennes entreprises européennes de l'Internet, qui s'appuient sur la publicité comportementale en ligne, seront impactées de manière significative par rapport aux géants de l'Internet qui peuvent fonctionner indépendamment des cookies tiers. Nous encourageons donc la Commission à maintenir les dispositions actuelles en vertu de la directive «vie privée et communications électroniques».

3. ANNUAIRES ACCESSIBLES AU PUBLIC

Les paragraphes 1 et 3 de l'article 15 introduisent une distinction entre les utilisateurs finaux qui sont soit des personnes physiques soit des personnes morales au regard de leur inclusion dans les annuaires accessibles au public. Cette distinction concerne principalement le consentement. En effet, les utilisateurs finaux qui sont des personnes physiques devront donner leur consentement explicite pour voir leurs informations répertoriées (opt-in) alors que les utilisateurs finaux qui sont des personnes morales verront leurs données systématiquement publiées sauf s'ils émettent une opposition formelle auprès du fournisseur d'annuaire accessible au public (opt-out). Nous comprenons la volonté de la Commission de renforcer la protection des utilisateurs finaux qui sont des personnes physiques. Néanmoins, certaines professions, telles que les avocats, bénéficient du statut d'indépendant. Ces professionnels s'enregistrent auprès du registre du commerce et des sociétés en leur nom propre. Seront-ils considérés comme personnes physiques ou comme personnes morales? Nous demandons à la Commission d'apporter des clarifications quant à la catégorisation de ce type de professions.

Par ailleurs, dans le cas des utilisateurs finaux qui sont des personnes morales, les fournisseurs d'annuaires accessibles au public publient les informations générales de la société telles que l'adresse ou le numéro de téléphone mais ils publient également les coordonnées des dirigeants de ces sociétés. Nous comprenons que, d'après l'article 15 (2), les fournisseurs d'annuaires accessibles au public devront demander le consentement de ces dirigeants pour être autorisés à les publier conjointement avec les informations de la société. Nous serions reconnaissants si la Commission pouvait confirmer notre compréhension.

De plus, de nombreux annuaires historiques accessibles au public qui bénéficient d'un statut particulier, sont disponibles dans les États Membres. C'est le cas, par exemple, de l'annuaire géré par Editus Luxembourg S.A. D'après notre compréhension, pour être conforme à la proposition de la Commission, les fournisseurs d'annuaires accessibles au public devront demander a posteriori le consentement de chacun de leurs clients qui sont des personnes physiques y figurant déjà, ce qui représente une charge de travail considérable. Au regard du statut spécial de ces annuaires historiques, nous demandons à la Commission de prévoir une dérogation particulière permettant aux fournisseurs de ces annuaires de ne pas avoir à demander le consentement de tous les utilisateurs finaux qui sont des personnes physiques figurant dans ces annuaires, mais plutôt de les informer que leurs données personnelles sont publiées dans ces annuaires et de leur permettre de demander le retrait de l'annuaire (par le mécanisme de l'opt-out).

4. PROTECTION CONTRE LES SPAMS ET LES ACTES DE PHISHING

D'après le considérant 19, l'article 6 (3) b. de la proposition de règlement, et sa lecture conjointe avec l'article 36, point 2 et 3 du RGPD, impose des obligations drastiques aux fournisseurs et opérateurs de communications électroniques pratiquement impossibles à remplir pour pouvoir traiter le contenu des communications électroniques en transit avec le consentement éclairé de tous les utilisateurs finaux concernés. En effet, les attaques par emails «phishing» et «spam» ou SMS ont déjà fait trop de victimes, les consommateurs n'ayant pas été suffisamment sensibilisés aux risques liés à ces attaques. Ces emails «phishing» et «spam » ou SMS surchargent le réseau de communications électroniques et contiennent très souvent un numéro surtaxé à rappeler ou un lien malicieux pour compromettre les téléphones mobiles et les appareils et lancer des attaques depuis ces appareils. Il nous semble dès lors pertinent que les fournisseurs de services de communications électroniques aient la possibilité d'analyser ces messages, de les mettre en quarantaine et d'informer les utilisateurs finaux du statut particuliers de ces emails ou SMS. Il reste, cependant, de la responsabilité des utilisateurs finaux de valider le statut de ces communications électroniques. Pour ce faire, FEDIL-ICT plaide pour une démarche volontaire de la part des utilisateurs finaux leur permettant de souscrire à un service de «screening» du contenu de leurs communications électroniques afin de déterminer s'il s'agit de «phishing» ou de «spam». Il est évident que cela nécessitera l'accès, par les fournisseurs de services de communications électroniques, à la messagerie des utilisateurs finaux mais également au contenu de leurs communications électroniques. Suivant le texte actuel, les fournisseurs de services de communications électroniques devront obtenir le consentement de tous les utilisateurs finaux en bonne et due forme conformément à la définition de l'article 9 (1) du RGPD. De plus, les fournisseurs devront consulter l'autorité de contrôle au préalable lors du traitement de ce type de données suivant les dispositions de l'article 36 du RGPD.

FEDIL-ICT souhaite ici proposer une alternative à la proposition actuelle: un système de screening débutant par une surveillance globale sans reconnaissance aucune d'un destinataire ou toute analyse du contenu, ne nécessitant de ce fait pas le consentement des utilisateurs finaux. Par la suite, l'implémentation d'une logique suivant la configuration d'un arbre de décision conduira le système à déclencher les opérations permettant le blocage des emails ou SMS suspectés en dernière étape. C'est avec la réalisation de différentes étapes que des indices sur une activité préjudiciable pour les utilisateurs finaux, et donc pour les opérateurs eux-mêmes, sont découverts. Grâce aux indices en résultant, une activité anormalement élevée provenant

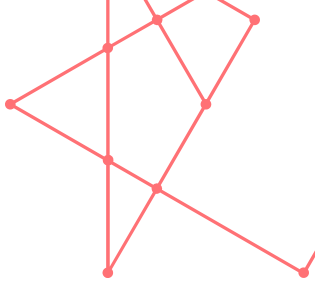
d'un seul et même numéro ou origine est décelée et des mesures complémentaires de contrôle appropriées seraient prises pour passer à des stades de surveillance plus individualisés. Ce ne serait qu'au dernier stade indiquant que des envois sont malveillants, en général, en raison du nombre extrêmement important envoyé, qui ne peut être que l'œuvre d'une machine, que le contenu des communications électroniques est vérifié pour éviter toute erreur. Si les emails ou SMS sont confirmés comme étant malveillants, l'expéditeur sera bloqué pour éviter un étalement de l'impact à l'ensemble des clients avec transmission d'un communiqué à la clientèle via le site web de l'opérateur ou du fournisseur de services ou par un autre canal.
FEDIL-ICT prie la Commission de bien vouloir prendre sa proposition en considération et d'apporter les modifications nécessaires au texte permettant aux fournisseurs de services de communications électroniques de procéder tel que décrit ci-dessus.

5. CONSENTEMENT

Nous nous permettons de revenir sur la possibilité pour les utilisateurs finaux de retirer leur consentement à tout moment conformément à l'article 7 (3). L'article 9 (3) précise que cette possibilité doit leur être rappelée tous les six mois. Or, que ce soit dans le cas d'utilisateurs finaux qui sont soit des personnes physiques soit des personnes morales, si ceux-ci sont liés aux fournisseurs de services de communications électroniques par un contrat qui court sur une certaine durée, qu'advient-il de ce contrat lorsque les utilisateurs finaux souhaitent retirer leur consentement?

Les clauses contractuelles régissent, en effet, la relation entre les utilisateurs finaux et les fournisseurs de services de communications électroniques pour une durée définie au préalable dans ce contrat. Nous estimons que le droit de retrait du consentement ne doit pas se faire au préjudice de la réalisation contractuelle de ce qui est dû initialement. Nous demandons à la Commission de préciser qu'un contrat établi pour une durée déterminée entre les utilisateurs finaux et les fournisseurs de services de communications électroniques ne puisse pas être rompu pour la cause de retrait du consentement tel que stipulé à l'article 9 (3). Il sera alors toujours nécessaire pour les fournisseurs de services de communications électroniques d'obtenir le consentement pour les cas de traitements autorisés de données et de contenu de communications électroniques selon l'article 6 (2) c. et (3) a. et b. Cependant, nous demandons à la Commission la possibilité de stipuler dans le contrat que ce consentement est obtenu pour la durée contractuelle.

En outre, cela pose la question de la nature des règles proposées à savoir si elles sont d'ordre publicou non. En effet, si tel est le cas, nous demandons à la Commission d'autoriser les utilisateurs finaux à renoncer à ces règles par le biais de l'introduction de conditions générales de vente (CGV), bien entendu suffisamment exhaustives, leur permettant de donner leur consentement de manière libre, spécifique, éclairée et univoque pour la fourniture des services de communications électroniques prestés par le fournisseur. Ces CGV régiraient la relation pour la durée du contrat et lèveraient, entre autres, la possibilité de retirer son consentement à tout moment. L'idée derrière cette proposition, est d'établir, dès le début de la relation commerciale entre les utilisateurs finaux et les fournisseurs de services de communications électroniques, ce que souhaitent ou non les utilisateurs finaux et de ne plus revenir dessus par la suite tant que la relation commerciale perdure et que le traitement se poursuit. Au regard de la proposition actuelle, nous comprenons que les fournisseurs de services de communications électroniques ne seront plus en mesure de prester les services dès lors que le consentement est retiré. Qu'en est-il alors du respect des délais de préavis établis dans le contrat? Nous serions reconnaissants si la



Commission pouvait apporter des clarifications sur ce point.