

Paris, le 7 septembre 2016

NOTE DES AUTORITÉS FRANÇAISES

Objet : Révision de la directive 2002/58/CE « vie privée et communications électroniques »

Les autorités françaises saluent, à titre liminaire, l'ambition affichée par la Commission européenne de mener une réflexion approfondie sur la pertinence et l'efficacité de la directive 2002/58/CE « vie privée et communications électroniques » ainsi que son articulation avec le règlement (UE) 2016/679 relatif à la protection des données à caractère personnel.

Les autorités françaises considèrent que cette réflexion devrait être guidée par deux principes essentiels :

- Simplifier et se limiter aux sujets essentiels

La directive 2002/58/CE telle que modifiée par la directive 2009/136/CE porte sur le « traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques ». Il est primordial d'examiner dans quelle mesure ses dispositions doivent évoluer, compte-tenu de l'adoption en avril 2016 du règlement (UE) 2016/679 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, dont le champ d'application inclut le secteur des communications électroniques. Cet examen doit permettre d'identifier, au cas par cas, les besoins spécifiques non couverts par le nouveau règlement et de supprimer les dispositions devenues obsolètes ou redondantes. La révision de la directive « vie privée et communications électroniques » doit donc être l'occasion d'une simplification juridique répondant à un impératif de lisibilité du droit et de sécurité juridique des acteurs économiques. Elle doit néanmoins préserver et adapter la protection assurée par la directive sur ces données particulières que constituent les données de communication afin d'éviter l'émergence de services fondés sur l'analyse des communications des personnes en méconnaissance du respect des communications, droit fondamental inscrit à l'article 7 de la Charte des droits fondamentaux de l'Union européenne.

- Principe d'équité et de neutralité technologique : « à services équivalents, règles équivalentes »

Le second axe de révision de la directive 2002/58/CE répond à l'impératif de soumettre au même encadrement tous les services, quel que soit le vecteur technologique utilisé, qui délivrent des services fonctionnellement équivalents à des services de communications électroniques.

Aujourd'hui, de nombreux services en ligne (services de téléphonie sur IP, réseaux sociaux, services de messagerie en ligne, etc.) sont les supports de nouvelles formes de communications

électroniques. Le récent rapport du BEREC (« *Body of European Regulators for Electronic Communications* ») paru en février 2016 montre que certains services par contournement fournissent les mêmes usages que les services de communications électroniques (et, notamment des services de correspondances privées). Pour garantir l'équité du cadre, pour préserver la compétitivité des acteurs européens ainsi que pour assurer le respect des acquis et des valeurs de l'Union, il est crucial que cet exercice de révision de la directive 2002/58/CE permette une réflexion et des avancées significatives afin de garantir une égalité des conditions de concurrence (« *level playing field* ») entre tous les acteurs fournissant des services et usages équivalents. C'est d'ailleurs la voie que la Commission a suggéré d'emprunter dans sa communication du 25 mai 2016 relative aux plateformes en ligne.

Cet alignement devrait être l'occasion de soumettre les services de communications par contournement à tout le moins aux obligations essentielles qui auraient vocation à demeurer dans la directive 2002/58/CE, dont le principe de confidentialité des communications, ainsi que la possibilité pour les Etats membres d'imposer la mise en œuvre des moyens nécessaires à la réalisation des interceptions judiciaires.

Au-delà de l'application de règles équivalentes à des services équivalents, l'exigence d'une protection cohérente des utilisateurs invite à s'interroger sur l'application de certaines dispositions de la directive 2002/58/CE (en particulier celles relatives au traitement des données de trafic et de localisation, cf. *infra*) aux services en ligne autres que des services de communications équivalant à des services de communications électroniques.

Dans le cadre de ces deux principes, les autorités françaises considèrent que la révision de la directive 2002/58/CE « vie privée et communications électroniques » devrait s'effectuer selon les grandes lignes précisées ci-dessous. Elles pourront néanmoins être appelées à évoluer à la lumière de la décision que rendra la Cour de justice de l'Union européenne (CJUE) à l'automne 2016 relativement aux questions préjudicielles C203/15 et C698/15, qui concernent l'interprétation de la directive 2002/58 sur la question de l'existence et de l'encadrement d'une obligation générale de conservation des données.

I – Sur le champ d'application

L'égalité de traitement entre les services par contournement et les services de communication électronique devrait concerner l'ensemble des règles qui subsisteraient dans la directive révisée, en particulier : confidentialité des communications (article 5), traitement des données relatives au trafic et à la localisation (article 6 et 9), droit de ne pas recevoir de facture détaillée (article 7) et consentement préalable obligatoire aux communications non sollicitées (article 13).

Par ailleurs, à l'instar des avancées significatives découlant de l'adoption du règlement européen relatif à la protection des données à caractère personnel en ce qui concerne la portée territoriale de la norme européenne, il est aussi important que la révision de la directive 2002/58/CE examine attentivement la question du champ d'application territorial. En effet, s'agissant notamment d'opérateurs de services par contournement ne disposant pas nécessairement d'établissement stable sur le territoire de l'Union européenne, la question de la capacité de la directive à appréhender ces acteurs est critique. Il s'agit d'une condition essentielle à l'efficacité du nouveau texte. Pour y remédier, la désignation obligatoire par ces opérateurs d'un représentant sur le territoire de l'Union, à l'image de ce qui est prévu à l'article 27 du règlement (UE) 2016/679 relatif à la protection des données à caractère personnel, pourrait être opportune.

De la même façon, s'agissant des prérogatives des régulateurs des États membres, les autorités françaises veilleront tout particulièrement à ce que, dans les cas où les règles du texte ne sont pas respectées par certains services de communications électroniques, la compétence du régulateur national reste pleine et entière, dès lors que les droits à la protection de résidents français sont

affectés, y compris dans les cas où l'opérateur en question disposerait d'un établissement principal situé sur le territoire d'un autre État membre.

II – Sur les dispositions au cœur du projet

a) La confidentialité des communications et le secret des correspondances

Ce principe doit être réaffirmé et appliqué à tous les services permettant l'acheminement de correspondances privées. Ce principe est un fondement de la confiance des utilisateurs dans les outils numériques (et notamment la téléphonie et la messagerie). C'est également une composante clef du respect des articles 7 (relatif à la protection de la vie privée et familiale), 8 (protection des données à caractère personnel) et 11 (relatif à la liberté d'expression) de la Charte des droits fondamentaux de l'Union européenne.

Il ne doit néanmoins pas empêcher certains usages légitimes comme l'antispam, le maintien de la sécurité du réseau, la détection de maliciels, la détection et la prévention de failles de sécurités... À cet égard, la Commission européenne pourrait s'inspirer du dispositif adopté dans le cadre du projet de loi pour une République numérique, qui définit les règles applicables aux différentes catégories de services et prévoit des mécanismes de consentement régulier pour certains services.

La piste d'une « sphère de vie privée » au sein de laquelle certaines communications pourraient être exploitées pour d'autres services, au seul bénéfice de l'utilisateur, peut également constituer une piste intéressante.

b) Le régime des cookies et autres traceurs

Concernant la confidentialité des informations, les autorités françaises sont attachées à un juste équilibre entre le besoin de modération à l'utilisation des cookies ou autres traceurs à l'insu des utilisateurs et la nécessité de préserver les espaces d'innovation et des nouveaux usages numériques pour les acteurs. Il apparaît notamment que la règle actuelle (recueil du consentement préalable au dépôt de certains cookies) est interprétée de manière plus ou moins stricte entre les différents États membres : il conviendrait de s'assurer d'une harmonisation européenne des pratiques à ce sujet tout en gardant des dispositions neutres technologiquement. À cet égard, il serait important de disposer de normes européennes permettant aux cookies de ne pas perturber la navigation sur Internet (élaborées à partir de l'exigence essentielle d'empêcher le blocage de l'accès aux sites). Les organismes européens de normalisation pourraient être mandatés par la Commission pour élaborer ces normes.

Sur le fond, il convient sans doute de privilégier une approche qui informe plus clairement l'utilisateur sur le nombre et les finalités des cookies et autres traceurs (par exemple, par l'affichage obligatoire d'un nombre de cookies et traceurs installés sur la page) à une approche fondée sur le consentement, qui a montré sa limite, même si elle reste nécessaire pour certaines finalités. En tout état de cause, il apparaît aux autorités françaises que les règles établies en 2009 par la directive n'ont pas apporté les satisfactions nécessaires.

c) Données relatives au trafic et données de localisation

En ce qui concerne le traitement des données de localisation et de trafic collectées, les autorités françaises sont attachées à ce que ces données très sensibles fassent l'objet d'une protection spécifique, notamment via le mécanisme de l'anonymisation. Les données non-anonymisées ne peuvent continuer à être utilisées que pour les utilisations strictement définies dans la directive actuelle : transmission d'une communication ou, pendant une durée limitée, facturation. En dehors

de ces usages, le consentement préalable doit rester nécessaire pour la fourniture de services à valeur ajoutée.

Les autorités françaises estiment par ailleurs souhaitable d'examiner la possibilité de soumettre l'ensemble des données de localisation aux obligations prévues par l'article 9 de la directive (il pourrait par exemple s'agir des données de localisation transmises par les véhicules connectés aux constructeurs ou dans certains lieux publics comme les aéroports ou des données de localisation transmises par le système GPS).