Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Le 21 novembre 2011

AVIS N° 6 DU CONSEIL NATIONAL DU NUMÉRIQUE RELATIF À LA PARTIE RÉGLEMENTAIRE DE LA TRANSPOSITION DE LA RÉVISION DU PAQUET TÉLÉCOM

L'ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques a procédé à la transposition dans le Code des postes et des communications électroniques des directives européennes 2009/136/CE et 2009/140/CE du 25 novembre 2009, dites « révision du paquet télécom ».

Dans le prolongement de cette ordonnance, trois projets de décret ont été rédigés destinés à préciser notamment :

> les règles d'établissement et d'exploitation des réseaux ouverts au public et de fourniture au public de services de communications électroniques ;

> les règles relatives au traitement de données à caractères personnel, à la sécurité et à l'intégrité des réseaux et des services ;

> les règles relatives à l'information et à la protection des utilisateurs ;

> les règles relatives à l'acheminement et à la localisation des appels d'urgence, à la transmission des messages d'alertes et d'information des pouvoirs publics afin d'avertir le public de dangers imminents.

Le ministre en charge de l'Économie numérique a saisi le Conseil national du numérique pour avis sur ces trois projets de décrets. Ces textes ont appelé de la part du CNN les commentaires suivants.

Sur les principes posés par le Conseil national du numérique

Dans son avis du 23 mai 2011, le Conseil national du numérique a eu l'occasion d'indiquer plusieurs principes. En ce qui concerne la neutralité des réseaux, le CNN relevait que le projet d'ordonnance prévoyait un cadre juridique adéquat permettant une information complète et transparente du consommateur ; cette information portant à la fois sur les restrictions à l'accès mais également sur les politiques de gestion de trafic mises en œuvre par les opérateurs.

En donnant ainsi au consommateur une information transparente et, en parallèle, en confiant au ministre et à l'Arcep les missions de veiller à l'absence de discrimination ainsi qu'à la capacité des utilisateurs finals à accéder à l'information, le projet d'ordonnance permettait d'établir des règles claires afin d'éviter tout risque d'atteinte au principe de neutralité des réseaux. Ces principes ont été repris dans l'ordonnance finalement adoptée.

CNNum
Conseil National du Numérique

Dans son avis en date du 17 juin 2011, le Conseil national du numérique a rappelé qu'il reste attaché au fait que la lutte contre les contenus et les comportements illicites diffusés et propagés sur l'internet demeure un objectif important. En cela, la participation des acteurs de l'internet à cette lutte s'inscrit totalement dans la démarche d'une coresponsabilité prônée lors du eG8 Forum et reprise dans la déclaration finale du G8 des 26 et 27 mai 2011.

Néanmoins, cette participation des acteurs de l'internet à la lutte contre la cybercriminalité doit s'inscrire dans un certain nombre de principes :

> elle doit être proportionnée et subsidiaire : le premier responsable d'un contenu ou d'une activité sur l'internet demeure l'auteur de ce contenu ou de cette activité. L'implication des intermédiaires de l'internet ne peut se faire que de manière subsidiaire ;

> elle doit être harmonisée : dans le cadre de la construction d'un marché unique au plan européen, et plus largement, dans le souci d'assurer aux entreprises françaises l'absence de barrières – notamment réglementaires – au développement de leur activité, toute mesure s'appliquant à ces intermédiaires doit être harmonisée, *a minima*, au plan européen ;

> elle doit s'inscrire dans le respect des principes constitutionnels largement reconnus et en particulier, la liberté du commerce et de l'industrie, la protection des données personnelles et surtout la liberté d'expression et de communication impliquant celle de recevoir et d'émettre des informations.

Sur le décret portant transposition du nouveau cadre réglementaire européen dans le Code des postes et des communications électroniques et portant renforcement de la sécurité des moyens d'interception des communications électroniques

Sur l'article 4 relatif à la séparation fonctionnelle

Concernant les obligations imposées aux opérateurs puissants sur un marché et dans le prolongement de l'ordonnance du 24 août 2011, la transposition des directives européennes est complétée par le projet de décret R. 9-5 du Code des postes et des communications électroniques relatif aux éléments justifiant l'imposition par l'Arcep de l'obligation de séparation fonctionnelle. Ce remède introduit par le nouveau cadre est d'une grande importance.

Le Conseil national du numérique recommande donc que le projet de décret soit modifié afin de garantir une transposition plus précise des dispositions européennes. En particulier, le projet d'article R. 9-5 devrait être modifié afin de prévoir « *une analyse de l'effet escompté sur […] ainsi que* ***sur les incitations à l'investissement*** *dans un secteur dans son ensemble* ».

De même, le projet d'article R. 9-5 institue « *une analyse de l'effet escompté sur la concurrence, notamment pour les autres acteurs, ainsi que des effets potentiels pour les consommateurs* ». Le Conseil national du numérique recommande de prévoir que cette analyse s'opère « ***sur les autres acteurs du marché****, ainsi que des effets potentiels pour les consommateurs* ».

Sur l'article 26 relatif à la conservation des données relatives aux mots de passe par les intermédiaires de l'internet

Aux termes du II de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, « *les personnes mentionnées aux 1 (fournisseurs d'accès) et 2 (hébergeurs) du I détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires* ».

En application de cette disposition, le décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création de contenu en ligne a fixé la liste des données devant être conservées par les intermédiaires de l'internet.

Parmi ces données, le 3° de l'article 1er du décret impose aux intermédiaires de conserver diverses « *informations fournies lors de la souscription d'un contrat par un utilisateur ou lors de la création d'un compte* », ces données ne devant être conservées « *que dans la mesure où les personnes les collectent habituellement* ».

Le g) du 3° de l'article 1er prévoit une obligation de conserver : « *le mot de passe ainsi que les données permettant de le vérifier ou de le modifier, dans leur dernière version mise à jour* ».

Souhaitée par les services d'enquête, cette conservation a été critiquée par plusieurs acteurs de l'internet et associations de défense des libertés au motif qu'elle avait pour effet d'obliger une conservation, dans une forme non cryptée, d'une donnée sensible et, d'autre part, que la communication de cette information pouvait porter atteinte au respect de la vie privée.

Le projet de décret soumis au CNN prévoit en son article 26 une modification de l'obligation pesant sur les prestataires de l'internet. Ainsi, la conservation et la communication des données seraient limitées aux « *données permettant de vérifier le mot de passe ou de le modifier, dans leur dernière version mise à jour* ».

La conservation et la communication du mot de passe sont donc supprimées ; seule subsiste l'obligation de conserver et de communiquer les informations permettant de vérifier le mot de passe ce qui vise, en pratique, les questions « secrètes » et les réponses associées.

Si la modification opérée répond à certaines craintes évoquées par les acteurs de l'internet, elle n'y répond qu'en partie. En effet, les intermédiaires de l'internet demeurent soumis à toutes les obligations issues de la loi du 6 janvier 1978 relative à l'informatique et aux libertés, et en particulier à des obligations de sécurité et de confidentialité des données qu'ils stockent. En cela, les intermédiaires de l'internet se doivent de respecter les prescriptions imposées par la loi notamment en matière de conservation, mais également de communication des données.

Or, l'article 6-II de la LCEN prévoit que l'obligation de conservation aux fins de communication aux autorités d'enquête ne porte que sur les données « *de nature à permettre l'identification de quiconque a contribué à la création d'un contenu* ». Or, le mot de passe et *a fortiori* les informations permettant de retrouver le mot de passe ne permettent pas de procéder à l'identification d'une personne.

Au contraire, et comme indiqué dans le projet de décret, la finalité des données collectées par l'intermédiaire est de « *vérifier le mot de passe ou de le modifier* », et donc en aucun cas d'identifier la personne elle-même. Certains de ces éléments collectés sont potentiellement des éléments de la vie privée de la personne physique (nom de la première petite amie, etc.) qui sortent du périmètre des données que les intermédiaires de l'internet sont autorisés à communiquer sur la base d'une réquisition judiciaire.

Communiquer ces données permettrait alors à la personne qui en serait destinataire de pouvoir accéder et/ou modifier le mot de passe d'un utilisateur et donc, potentiellement, permettrait d'accéder à des informations en dehors du cadre légal approprié.

En conséquence, le Conseil national du numérique recommande que l'article 26 du projet de décret supprime le g) du 3° de l'article 1er du décret du 25 février 2011.

Sur le projet de décret portant modification des obligations des opérateurs prévues par le Code des postes et des communications électroniques conformément au nouveau cadre réglementaire européen

Sur l'article 1er sur la certification des méthodes de mesure de la qualité de service

Cette disposition donne compétence à l'Arcep en matière de « *certification des méthodes de mesure de la qualité de service* », cette dernière ayant la faculté de demander une certification des méthodes mises en œuvre par les opérateurs.

Cette mesure, favorable au consommateur, s'inscrit dans le principe de transparence prévu par l'ordonnance de transposition de la révision du paquet télécom. En effet, la qualité de service proposée par les opérateurs permettra au consommateur final d'avoir connaissance de toute mesure qui aurait pour objet ou pour effet de limiter la qualité de l'accès aux services proposés sur internet.

Pour autant, il convient de rappeler qu'une certification repose sur la vérification par un tiers de la conformité d'un produit ou d'un service à un cahier des charges préalablement établi et validé. À ce titre, une contribution de l'ensemble des parties prenantes à l'élaboration du cahier des charges et aux méthodes de certification semble nécessaire.

Le Conseil national du numérique estime qu'il peut être opportun que l'Arcep organise une consultation publique de l'ensemble des acteurs économiques et non économiques à l'élaboration de la méthode de certification des outils de mesure de la qualité des services proposés par les opérateurs.

En tout état de cause, il convient de rappeler que la mise en œuvre de cette mesure ne saurait avoir pour effet de créer de nouvelles sujétions aux opérateurs.

Sur l'article 2 relatif aux politiques de sécurité mises en œuvre par les opérateurs

Cette disposition modifie et complète l'article D. 98-5 du Code des postes et communications électroniques en prévoyant que « *l'opérateur met en œuvre une politique de sécurité relative au traitement des données à caractère personnel et prend les mesures nécessaires garantissant, pour le moins, que seules des personnes autorisées puissent avoir accès aux données à caractère personnel dans les cas prévus par des dispositions législatives et réglementaires et que les données à caractère personnel stockées ou transmises soient protégées contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelles et le stockage, le traitement, l'accès et la divulgation non autorisés ou illicites* ».

Renforçant la protection des données personnelles des utilisateurs, le Conseil national du numérique accueille de façon favorable cette disposition. En effet, celle-ci a pour objet et pour effet de demander aux opérateurs d'élaborer une politique de protection « interne » des données collectées.

Pour le Conseil national du numérique, outre la mise en place des outils techniques et des règles d'accès nécessaires, cette politique devra se faire au travers d'une sensibilisation des équipes des opérateurs aux règles applicables et aux limites posées par les textes en vigueur.

Elle devra, notamment, rappeler les possibilités offertes par le droit aux autorités d'enquête et le cadre applicable aux demandes adressées par celles-ci. Cette politique permettra notamment de s'assurer que la communication tant dans sa forme, que dans le contenu transmis, respecte ledit cadre législatif et réglementaire.

Par ailleurs, l'article D.98-5 est modifié en prévoyant les nouvelles obligations pesant sur les opérateurs pour assurer l'intégrité de leurs réseaux. Notamment, l'opérateur est tenu de prendre « les *mesures utiles pour assurer la sécurité et l'intégrité des dispositifs intégrés aux équipements terminaux nécessaires à l'identification et à l'authentification des utilisateurs pour la fourniture de services de communications électroniques* ».

L'opérateur assure la responsabilité des dispositifs d'identification et d'authentification. En conséquence, afin d'assurer cette obligation de sécurité et d'intégrité, le Conseil national du numérique recommande que l'arrêté ministériel prévu au D.98-5 précise les conditions dans lesquelles **les dispositifs fournis répondent à un niveau approprié de sécurité et d'intégrité, et les conditions dans lesquelles cela est vérifié le cas échéant à la charge des fournisseurs de services. Une telle charge ne peut être imposée aux opérateurs puisque ces derniers ont l'obligation de connecter les équipements dès lors qu'ils sont conformes aux exigences essentielles**.

Sur l'article 19 sur le portage des numéros

L'article 19 du projet de décret modifie les dispositions de l'article D. 406-18 du Code des postes et communications électroniques en matière de portage des numéros. En particulier, cet article fixe les conditions de calcul du délai de portage maximum pour l'abonné, le portage étant le nombre de jours calendaires ouvrables entre l'obtention par l'opérateur receveur de la confirmation de l'éligibilité de la demande de conservation du numéro et, d'autre part, le portage effectif du numéro.

Or, conformément au cadre règlementaire fixé par l'Arcep, l'opérateur receveur ne connaît pas d'avance la date à laquelle la confirmation de l'éligibilité de la demande de conservation lui parviendra, l'Arcep n'imposant à l'opérateur donneur que des délais maximums de réponse pour confirmer à l'opérateur receveur l'éligibilité de la demande de conservation du numéro.

Il conviendrait donc de prendre comme point de départ la date de fin de la période allouée à l'opérateur donneur pour envoyer la confirmation de l'éligibilité de la demande de conservation du numéro.

Sur le projet de décret pris pour l'application de l'article 34 bis de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et relatif à la prévention et à la notification des violations des données à caractère personnel

Dans le prolongement de l'ordonnance, le décret complète la transposition de la révision du Paquet Télécom en prévoyant la procédure de notification des violations de données personnelles à la Commission nationale de l'informatique et des libertés et dans certains cas à l'abonné ou particulier victime de cette violation, ainsi que la procédure d'information de la Cnil sur les mesures de protection technologiques mises en œuvre par l'opérateur afin de rendre les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès.

En la matière, le projet de décret précise les conditions dans lesquelles la notification aux personnes concernées peut ne pas être faite en raison du caractère approprié des mesures de protection technologiques « proposées » par l'opérateur.

Ainsi, l'article 91-5 ajouté par le projet de décret prévoit une procédure d'information et de validation par la CNIL des mesures de protection technologiques. Cette procédure impose à la Cnil d'apporter une réponse dans un délai de quatre mois. À défaut de réponse, l'avis de la Cnil sera considéré comme étant un avis négatif.

Les autorités ont souhaité dans le dispositif de cette nouvelle obligation que les acteurs, agissent avec promptitude, dans un environnement extrêmement évolutif, vis-à-vis des utilisateurs de leurs services. Le dispositif portant sur une des conditions permettant de ne pas notifier aux utilisateurs en cas de validation de la mesure technologique mise en œuvre doit pouvoir répondre à cette même exigence de temps. Il semble nécessaire que le temps du dialogue à instaurer avec la Cnil dans le cadre de la procédure prévue aux articles 91-4 et 91-5 puisse revêtir le caractère raisonnable : il est manifeste que faire une notification aux personnes plus de quatre mois après un fait déclencheur en raison de la non-validation des mesures prises ou proposées par la Cnil ne peut que créer confusion et réaction contreproductive voire inadéquate.

Le Conseil national du numérique recommande ainsi que le projet de décret réduise utilement le délai d'examen du dossier par la Cnil de quatre à deux mois et qu'au terme de ce délai d'examen, l'absence d'avis de la Cnil soit considéré comme étant un avis positif.