

Mise en conformité des services internet en libre accès aux exigences de la loi Informatique et Libertés : les précautions à prendre

[DONNEES PERSONNELLES]

Communiqué de la CNIL du 22 décembre 2014

Dans le cadre de son programme annuel de contrôle, la CNIL s'est intéressée aux établissements publics ou privés proposant des bornes Wi-Fi ou internet en libre accès. Elle a estimé que les manquements relevés à l'occasion de ces contrôles justifiaient un rappel public des mesures qui doivent être mises en œuvre pour se conformer à la loi Informatique et Libertés.

1. **Conservation des données de trafic.** En mettant à disposition du public des services d'accès au réseau internet, les établissements agissent en qualité d'opérateurs de communications électroniques et sont par conséquent soumis aux règles édictées par le Code des Postes et Communications Electroniques (CPCE). A ce titre, ils doivent se conformer aux obligations de conservation des données prévues par l'article L. 34-1 du CPCE aux termes duquel l'opérateur doit par principe effacer ou rendre anonymes toutes données relatives au trafic, à savoir les « *données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou en vue de sa facturation* » telles que les logs de connexion, les adresses IP, la date et l'heure de connexion.

Cependant l'article L. 34-1 du CPCE prévoit un certain nombre d'exceptions permettant de retarder l'anonymisation des données de trafic dans le but de permettre la recherche et la poursuite d'infractions pénales. Ces données de trafic doivent être conservées un an à compter du jour de leur enregistrement et être communiquées aux autorités habilitées à leur demande (Article R. 10-13 du CPCE).

Or, la CNIL a constaté lors des contrôles que la majeure partie des établissements proposant des points d'accès internet conservaient des données portant sur *le contenu* des correspondances échangées ou sur *les informations consultées* par les utilisateurs en violation des dispositions du CPCE. La CNIL rappelle donc que seules les données de trafic peuvent être conservées.

Le fournisseurs de services doivent en outre veiller, d'une part, à appliquer une durée de conservation limitée à un an pour les données de trafic, délai au-delà duquel elles devront être anonymisées et, d'autre part, à supprimer régulièrement les autres données.

2. **Confidentialité et sécurité des données.** Les opérateurs de communication électronique ont une obligation générale de sécurité (D 98-5 III du CPCE). Ils doivent mettre en œuvre tous les moyens nécessaires afin de protéger leur réseau et assurer la sécurité des communications. Ils doivent également prendre les mesures techniques propres à assurer la protection, l'intégrité et la confidentialité des données à caractère personnel des utilisateurs.

La CNIL a relevé plusieurs lacunes sur la protection des réseaux utilisés par les organismes contrôlés dues à l'absence de chiffrement des réseaux wifi, l'absence ou la faiblesse des mots de passe permettant l'accès au système et la possibilité de prendre le contrôle des postes via une clé USB.



société d'avocats

Pour y remédier, la CNIL rappelle que les opérateurs doivent inclure une clause relative à la sécurité des données dans les contrats conclus avec les prestataires réseaux et adopter des mesures de sécurité plus strictes. Elle préconise notamment de (i) sécuriser les accès aux journaux de connexion, (ii) d'assurer la robustesse des mots d'accès au système d'exploitation et (iii) de limiter la durée de stockage des documents en attente d'impression pour éviter leur divulgation à des tiers.

3. **Information des utilisateurs.** Les contrôleurs de la CNIL ont observé que les utilisateurs des services n'étaient pas suffisamment informés sur les modalités de traitement de leurs données. Aussi, elle recommande que cette information soit fournie sur le formulaire d'inscription au service ou, à défaut, par voie d'affichage ou dans une charte informatique. En tout état de cause, les utilisateurs doivent être en mesure d'exercer gratuitement (i) leur droit d'accès aux données à caractère personnel les concernant, ainsi que (ii) leur droit de rectification ou de suppression de celles-ci. Les fournisseurs de services doivent donc prévoir des procédures de gestion spécifiques pour ces demandes.
4. **Recours limité aux outils de surveillance.** Au cours de leurs opérations de contrôle, les agents de la CNIL ont enfin relevé l'utilisation d'outils de surveillance par les fournisseurs de services aux fins d'assurer la sécurité des postes informatiques, la gestion des tarifications et les impressions. Le recours à ces outils est déconseillé par la CNIL. En effet, ils permettent un contrôle de l'historique de navigation et un contrôle à distance de l'ordinateur utilisé pouvant donner accès à de très nombreuses informations sans rapport avec la finalité poursuivie (ex : identifiants-mots de passe, numéros de compte bancaire, etc). En tout état de cause, en cas d'utilisation de ces outils, un paramétrage limité doit être prévu aux fins d'éviter toute collecte excessive de données.

L'ensemble des établissements offrant des espaces publics de connexion à l'internet (hôtels, restaurants, bibliothèques, municipalités, gares, etc.) devront donc revoir leurs pratiques et adopter des procédures de gestion plus strictes de leurs services. Ces opérations de refonte devront être menées à grande échelle. Selon le cabinet d'étude iPass, spécialisé dans les réseaux Wi-Fi, la France est le pays qui dispose à ce jour du plus grand nombre de bornes internet sans fil dans le monde (plus de 13 millions).

Sabine DELOGES