Wifi en libre accès : conseils pour ne pas se faire épingler par la Cnil pour « des manquements récurrents »

	Wifi en accès libre : conseils pour ne pas se faire épingler par la Cnil pour « des manquements récurrents »

La Commission nationale de l'informatique et des libertés (Cnil) a de bons côtés, parmi lesquels sa volonté inébranlable de garder la pêche. Chaque jour que Dieu fait, elle constate des entorses aux règles qu'elle est censée faire respecter, mais ne se décourage pas.

Nouvel exemple : l'autorité administrative indépendante a contrôlé des points où internet est disponible en libre accès – restaurants, hôtels, bibliothèques – via le wifi ou des postes informatiques dédiés. Sans surprise, elle a découvert « des manquements récurrents » :
• de nombreux opérateurs « conservent des données portant sur le contenu des correspondances échangées ou des informations consultées (URL) alors qu'ils ne sont pas autorisés à le faire » ;
• ils ne doivent conserver que les données de connexion, pendant un an. Or, la plupart les gardent indéfiniment ;
• les utilisateurs sont mal informés ;
• plusieurs opérateurs utilisent « des outils de surveillance » des postes informatiques comme la « prise en main à distance » et le « contrôle de l'historique de navigation ». C'est-à-dire qu'ils ont accès, de fait à des données sensibles : « identifiants-mots de passe, numéros de compte bancaire, etc ». La Cnil aimerait qu'ils arrêtent.
• les réseaux wifi, sans chiffrement et facilement accessibles, sont de vraies passoires. Il n'est pas difficile d'en prendre le contrôle.
Plutôt que de paniquer devant tant d'amateurisme, la Cnil garde le cap et donne cinq conseils pour améliorer les choses.

Au restaurant, à l'hôtel ou dans les bibliothèques, il est souvent possible d'utiliser un réseau internet wi-fi ou des postes informatiques en libre accès.
La CNIL a décidé d'intégrer dans son programme annuel des contrôles la thématique de l'internet en libre accès. Elle a effectué plusieurs contrôles des modalités de mise en œuvre de ce type de service auprès d'organismes privés et publics.

Lors de ces contrôles, l'attention de la CNIL a principalement porté sur :
• le type de données collectées,
• leur conservation,
• le niveau d'information des utilisateurs
• la qualité des mesures de sécurité qui y sont associées.

Plusieurs manquements récurrents ont été identifiés lors de ces contrôles. Au vu de ces constations, la CNIL rappelle aux fournisseurs de services d'internet en libre accès les mesures à adopter pour se mettre en conformité.

1. Conserver seulement les données de trafic
Les organismes qui mettent à disposition du public un service de libre accès à internet (postes informatiques, wi-fi, etc.) sont considérés comme opérateurs de communications électroniques (OCE) et sont soumis aux obligations prévues à l'article L. 34-1 du code des postes et des communications électroniques (CPCE). A ce titre, ils doivent conserver les données de trafic répondant aux » besoins de la recherche, de la constatation et de la poursuite des infractions pénales » et destinées aux autorités légalement habilitées.
La CNIL a constaté lors des contrôles que de nombreux opérateurs de communication électronique conservaient des données portant sur le contenu des correspondances échangées ou des informations consultées (URLs) alors qu'ils ne sont pas autorisés à le faire (article L. 34-1 VI du CPCE consultable sur http://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070987&idArticle=LEGIARTI000006465770&dateTexte=&categorieLien=cid).
Les fournisseurs de service ne doivent pas collecter de telles données et supprimer celles qui auraient été conservées.

2. Définir une durée de conservation des données limitée et proportionnée
La plupart des fournisseurs de service conservent les données issues des journaux de connexion sans qu'aucune durée de conservation n'ait été définie.
Or, les données de trafic doivent être conservées pendant 1 an à compter du jour de leur enregistrement (Article R. 10-13 du Code des postes et des communications électroniques consultable sur http://legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006466369&cidTexte=LEGITEXT000006070987&dateTexte=20110909&oldAction=rechCodeArticle)
Les autres données collectées dans le cadre de l'offre d'internet en libre accès, telles que les informations d'abonnement, etc. doivent être supprimées régulièrement (article 6-5° de la loi n°78-17 du 6 janvier 1978 modifiée consultable sur http://www.cnil.fr/documentation/textes-fondateurs/loi78-17/#Article6) lorsqu'elles ne sont plus nécessaires (désinscription ou inutilisation prolongée de l'abonnement).

3. Fournir une information complète sur les traitements de données :
Les contrôleurs de la CNIL ont observé que l'information fournie aux utilisateurs des services d'internet en libre accès, ne s'avérait pas toujours satisfaisante, voire inexistante.
Les opérateurs de communication électronique doivent délivrer une information aux utilisateurs de leur service sur les modalités de traitement de leurs données (article 32 de la loi n°78-17 du 6 janvier 1978 modifiée). Le support de cette information doit être le formulaire d'inscription au service. A défaut, l'information doit être fournie par voie d'affichage, dans une charte informatique, etc. (Voir les modèles de mention d'information sur http://www.cnil.fr/vos-obligations/informations-legales/).
Par ailleurs, les opérateurs de communication électronique doivent prévoir des procédures de gestion des demandes d'accès, de rectification et de suppression des données par leurs utilisateurs (art. 38 à 40 de la loi n°78-17 du 6 janvier 1978 modifiée).

4. Veiller à la conformité des outils utilisés, notamment aux outils de surveillance :
Plusieurs opérateurs de communication électronique contrôlés utilisaient des outils de surveillance afin d'assurer la sécurité des postes informatiques, la gestion des tarifications, les impressions, etc.
L'utilisation de tels outils (consultation ou prise en main à distance, contrôle de l'historique de la navigation, etc.) est susceptible de donner accès à un grand nombre d'informations excessives au regard de la finalité pour laquelle elles sont collectées (identifiants-mots de passe, numéros de compte bancaire, etc). Le recours à de tels outils doit être évité ou un paramétrage limité doit être mis en place.

5. Assurer la confidentialité et la sécurité des données :
Plusieurs lacunes en termes de sécurité et de confidentialité ont été révélées lors des contrôles :
• L'absence de chiffrement des réseaux wi-fi ;
• L'accessibilité du BIOS (absence ou faiblesse du mot de passe) permettant de modifier la configuration basique du système ;
• La possibilité de prendre le contrôle de la machine en démarrant un système d'exploitation depuis une clé USB ; etc.
Pour y remédier, les opérateurs de communication électronique doivent inclure une clause relative à la sécurité des données dans le contrat conclu avec le prestataire réseaux (voir le modèle de clause de confidentialité sur http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/sous-traitance-modeles-de-clauses-de-confidentialite).
Par ailleurs, ils doivent adopter des mesures de sécurité afin de (voir les guides sur » La sécurité des données personnelles » sur http://www.cnil.fr/documentation/guides/) .

Au travers de missions de mise en conformité ou de formation d'un futur correspondant CNIL (Correspondant Informatique et Libertés dit aussi CIL), Denis JACOPINI se charge de mettre en conformité votre établissement avec la Loi Informatique et Libertés auprès de la CNIL.
Vous souhaitez vous mettre en conformité avec la CNIL, contactez-nous

---

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://rue89.nouvelobs.com/2014/12/22/wifi-libre-acces-cnil-epingle-manquements-recurrents-256697