Fournir un accès internet public : quelles sont vos obligations ?

14 mai 2024

L'utilisation d'ordinateurs situés dans des espaces publics aménagés par les communes ou les cybercafés devient une pratique courante. Les responsables de ces espaces publics ont l'obligation de conserver les données de trafic.

De nombreux espaces offrent un accès internet à leurs utilisateurs : hôtels, restaurants, médiathèques, musées, transports, etc. Les responsables de cette fourniture d'accès sont soumis à des obligations légales de conservation des « données de trafic » et au respect des principes de la protection des données.

Qui est concerné par ces obligations ?

Les organismes qui offrent un accès internet au public, tels que les communes, les bars, les restaurants, les cafés, les fast-foods, les trains, les hôtels, etc.

Les « données de trafic », qu'est-ce que c'est ?

Les « données de trafic » sont les informations techniques qui sont créées lorsqu'on utilise un réseau comme Internet. Il s'agit par exemple de l'adresse IP permettant d'identifier l'appareil utilisé, de la date, de l'heure et de la durée de chaque connexion ou encore des données permettant d'identifier le destinataire d'une communication (par exemple le numéro de téléphone appelé).

En principe, ces informations doivent être effacées ou rendues anonymes. Cependant, certains textes légaux dérogent à cette règle en imposant aux organismes de **les conserver, pour permettre la recherche et la poursuite des infractions pénales par les services de police, gendarmerie et justice.**

Quelles données doivent-être conservées et pour quelles durées ?

Les données conservées, bien qu'essentiellement techniques, sont des données personnelles. Elles portent exclusivement sur l'identification des utilisateurs du réseau, sur les caractéristiques techniques et sur la localisation des appareils. Le contenu des messages échangés ou les informations consultées sur le réseau ne sont pas concernées.

Conformément à l'avis de la CNIL rendu le 7 octobre 2021, le principe de minimisation impose de **limiter la conservation aux données strictement nécessaires** au regard des finalités citées par l'article L34-1 du code des postes et des communications électroniques.

Les données relatives à l'identité civile de l'utilisateur

Les informations relatives à l'identité civile de l'utilisateur (nom, prénom, date et lieu de naissance de la personne, adresse postale, adresse courriel, numéro de téléphone) doivent être conservées pendant un délai de 5 ans.

Les autres informations fournies par l'utilisateur lors de la création d'un compte permettant d'accéder au réseau mis à disposition (identifiant, pseudonyme, données destinées à permettre à l'utilisateur de vérifier ou modifier son mot de passe) doivent être conservées pendant un délai de 1 an.

Les données techniques

Les données techniques permettant d'identifier la source de la connexion ou relatives aux appareils utilisés (adresse IP et port associé, numéro de l'identifiant, numéro d'identification, numéro de téléphone) doivent être conservées pendant un délai de 1 an.

Les données concernant la sécurité des réseaux et des installations

Les données suivantes peuvent être conservées pendant un délai de 3 mois maximum :

- les données permettant d'identifier l'origine de la communication ;
- les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;
- les données techniques permettant d'identifier le ou les destinataires de la communication ;
- les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs.

Quelles sont les droits des utilisateurs sur leurs données ?

Les utilisateurs disposent d'un droit d'accès et d'un droit de rectification. Ces droits s'exercent auprès des organismes fournissant l'accès à Internet, soit en contactant directement le responsable de l'organisme soit en contactant son Délégué à la protection des données s'il a été désigné.

Quelles mesures de sécurité doit prendre le responsable du lieu qui fournit un accès Internet ?

Le responsable doit sécuriser les réseaux wi-fi ouverts au public, en les séparant de son réseau interne et en utilisant un chiffrement à l'état de l'art (voir les recommandations de l'ANSSI sur ce dernier).

Il doit encadrer la sécurité des traitements de données personnelles, notamment en limitant leur accès aux seules personnes habilitées.

Le responsable doit également assurer la sécurité des réseaux à un niveau adapté au risque existant, prendre des mesures pour prévenir ou limiter les conséquences des atteintes à la sécurité pour les utilisateurs et assurer la sécurité des dispositifs nécessaires à l'identification et à l'authentification des utilisateurs pour la fourniture d'accès à Internet.

Et les employeurs ?

Les entreprises et les administrations fournissant un accès Internet, y compris par wi-fi, à leurs **employés** ne sont pas concernées par cette obligation de conservation.

Toutefois, un employeur a le droit de mettre en œuvre un dispositif de surveillance de l'activité internet de ses salariés (contrôle de la messagerie, des sites web consultés, etc.) dès lors qu'un certain nombre de garanties sont respectées, en particulier la définition d'un objectif précis, l'information des intéressés sur le système mis en œuvre, et l'inscription dans le registre des traitements.

Si l'employeur propose aux **visiteurs** dans ses locaux un accès au réseau Internet par wi-fi, il est alors tenu de respecter les obligations applicables décrites sur cette page.