

Loi du 23 janvier 2006, dite anti-terroriste. Que dit-elle ?

Qui est concerné par la loi ?

L'article L. 34-1 du CPCE indique que « *les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, effacent ou rendent anonyme toute donnée relative au trafic (...)* ». Le régime juridique applicable aux données relatives au trafic est également opposable aux « *personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit (...)* ».

Concrètement, l'obligation de conservation des données s'applique aux opérateurs de communications électroniques ainsi qu'à toute autre personne qui fournit un accès Internet dans le cadre d'une activité professionnelle. Les exploitants de « hotspots », tels que les cafés, les restaurants, les hôtels, les centres d'affaires, les cybercafés sont donc concernés, que l'activité de fournisseur d'accès soit effectuée à titre onéreux ou à titre gratuit et sans considération du fait qu'il s'agisse d'une activité principale ou secondaire.

Les personnes ainsi désignées sont soumises à l'obligation de principe tendant à effacer et à rendre anonymes les données techniques liées aux communications électroniques.

Quelles sont les données à conserver ?

Le CPCE indique que les données à conserver « *portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux* »

Tous les opérateurs doivent conserver certaines catégories de données techniques au cas où, dans le cadre d'une enquête **judiciaire**, les autorités chercheraient à identifier l'utilisateur des services proposés par l'opérateur.

Un décret est venu, le 24 mars 2006, préciser que :

- 1) les informations permettant d'identifier l'utilisateur ;
- 2) les données relatives aux équipements terminaux de communication utilisés ;
- 3) les caractéristiques techniques ainsi que la date, l'heure et la durée de chaque communication ;
- 4) les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ;
- 5) les données permettant d'identifier le ou les destinataires de la communication ;

doivent être conservées par l'opérateur pendant un an à compter du jour de leur enregistrement.

S'il s'agit du service téléphonique :

L'opérateur doit conserver en plus les données permettant d'identifier l'origine et la localisation de la communication.

Combien de temps doit-on conserver les données ?

Les obligations de conservation ne portent pas sur le contenu des communications échangées. Le cadre juridique a pour objet d'organiser les modalités d'accès aux données relatives au trafic, appelées également données techniques.

En ce sens, les dispositions de l'article L. 32 18° du CPCE indiquent que sont considérées comme données techniques « *toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou en vue de sa facturation* ». L'article R. 10-12 précise à son tour que ces données s'entendent des « *informations rendues disponibles par des procédés de communications électroniques susceptibles d'être enregistrées par l'opérateur à l'occasion des communications électroniques dont il assure la transmission et qui sont pertinentes au regard des finalités poursuivies par la loi* ».

Pour autant, le code prévoit un régime juridique dérogatoire qui impose la conservation pendant un an des données relatives au trafic dans le but de faciliter la recherche, la constatation et la poursuite des infractions pénales. La communication de ces données relèvera du mécanisme de la réquisition judiciaire.

La conservation des données peut être effectuée par l'opérateur ou confiée à des prestataires externes

S'agissant particulièrement de la prévention des actes de terrorisme, l'article L. 34-1-1 du CPCE prévoit le cas des réquisitions administratives qui permettent aux agents de la police et de la gendarmerie nationales habilités à cet effet d'obtenir communication de ces données auprès des opérateurs et des autres personnes mentionnées ci-dessus.

Quels sont les risques encourus pour le responsable légal ?

Il faut se référer à l'article 434-4, selon lequel "*est puni de **trois ans d'emprisonnement et de 45000 euros d'amende** le fait, en vue de faire obstacle à la manifestation de la vérité (...) de **détruire, soustraire, receler ou altérer un document public ou privé** ou un objet de nature à faciliter la découverte d'un crime ou d'un délit, la recherche des preuves ou la condamnation des coupables*".

Ce texte concernant les actes d'entrave à la justice, une personne tenue par la loi de communiquer des données techniques à la police, dans le cadre d'une enquête judiciaire, pourrait - si elle refusait de s'exécuter - être poursuivie sur le fondement de cet article.

Par ailleurs, ce dernier augmente les peines applicables lorsque l'infraction a été commise "*par une personne qui, par ses fonctions, est appelée à concourir à la manifestation de la vérité*". Les opérateurs (ou assimilés) pourraient, dès lors, être considérés comme exerçant de telles fonctions, puisque la loi met à leur charge une obligation particulière de coopération. Il ne peut donc être exclu qu'un juge retienne cette circonstance aggravante, notamment compte tenu du contexte sensible lié à la répression du terrorisme. Si tel était le cas, la peine serait de **cinq ans d'emprisonnement et 75000 euros d'amende**.

Quels sont les principes à respecter ?

La collecte et le traitement des logs doivent respecter certains principes, définis dans l'article 6 de la loi Informatique et Libertés. Cette collecte ne peut en effet se faire à l'insu des personnes concernées (principe de loyauté et licéité) et doit répondre à des finalités déterminées, explicites et légitimes. L'entreprise doit également répondre au principe de proportionnalité dans la collecte et le traitement, c'est-à-dire que « nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas proportionnées au but recherché ».

Pour être en conformité avec ces principes, il faut par conséquent que le fichier ait un objectif précis, que les informations exploitées dans ce fichier soient cohérentes par rapport à l'objectif défini et que ces dernières ne puissent être réutilisées de manière incompatible avec la finalité pour laquelle elles ont été collectées.

Les données doivent également respecter un principe d'exactitude et leur durée de conservation doit être cohérente avec les finalités définies.