NOTE JURIDIQUE

Clés de lecture juridique pour les opérateurs de télécommunications

Par Christel CHAUVEAU-SIMIOL
Juriste indépendante TERRI POLEIS
Mail : cchsimiol@terri-poleis.pro tel : 85 82 92

Fournisseurs de services de communications électroniques : responsabilités et enjeux

L'opérateur numérique : Responsable de traitement au sens de la loi informatique et Libertés (CNIL)

Fournisseurs de service de communications électroniques : responsabilité et enjeux

Internet constitue un nouvel espace de diffusion de contenus illicites, pouvant porter atteinte aux droits des tiers ou à l'ordre public.

La **responsabilité** dans la diffusion de contenus illicites des opérateurs numériques (opérateurs de réseaux, fournisseurs d'accès à Internet, hébergeurs) peut-elle être mise en cause ? puisqu'ils contribuent à la diffusion de contenus dangereux ?

D'un côté, ils ont un rôle clé à jouer dans la prévention la réduction des cyber-menaces, voire leur remédiation; mais de l'autre côté, ils peuvent être accusés de manipulation dans la circulation de données personnelles

En 1974, l'opinion publique s'alertait du projet SAFARI qui visait à interconnecter les fichiers des administrations sur les citoyens à partir du numéro de sécurité sociale (projet à l'origine de la loi 'informatique et Libertés' du 6 janvier 1978).

La vigilance semble plus encore nécessaire aujourd'hui avec le difficile contrôle des données personnelles déversées sur Internet, dans les réseaux sociaux et les systèmes d'information des entreprises.

En prenant pour référence des acteurs économiques aujourd'hui incontournables, les opérateur d'accès et de services de communications électroniques (ou opérateurs numériques), le présent exposé ne vise pas tant ici à définir ses obligations légales, que de lui proposer une feuille de route, capable de mettre en avant l'attachement à des valeurs éthiques, d'entreprise et d'intérêt général.

L'opérateur numérique pourra alors en faire un outil de marketing, clé de confiance vis à vis de ses partenaires, de ses employés et de ses clients.

Son cadre de responsabilité se définit dans la loi sur l'économie numérique (dite LCEN) et la loi Informatique et Libertés (loi CNIL).

L'opérateur numérique : prestataire technique ou gardien des libertés ?

Pour encadrer leur responsabilité, la **loi n°2004-575 du 21 juin 2004** ***pour la confiance dans l'économie numérique (LCEN),*** dans sa version applicable à la Nouvelle-Calédonie, a instauré un système de limitation de la responsabilité des opérateurs numérique.

Le point commun de ces intermédiaires se rapporte à un rôle purement technique afin de permettre l'accès à l'information. Par conséquent ils n'exercent en principe aucun droit de regard sur l'information qui circule.

La LCEN a tenté à la fois de définir pour chacun des 3 types d'opérateurs numériques le régime de responsabilité applicable à chacun.

A- Définitions

La loi LCEN identifie trois catégories d'intermédiaires techniques**, à savoir :**

1) **les opérateurs de réseaux qui réalisent le transport des données et du « caching [1] » (l'OPT en Nouvelle-Calédonie)**

[1] **Le caching** est le procédé par lequel certains éléments d'un site web (images, fichiers HTML,..) sont stockés par le navigateur au niveau du disque dur de l'internaute ou par le fournisseur d'accès au niveau de ses serveurs proxy. L'objectif du caching est que les fichiers ne transitent pas à nouveau sur le réseau lorsqu'un internaute revient sur une page déjà consultée ou que différents abonnés aux mêmes FAI consultent le même site. Source : www.definitions-webmarketing.com/Definition-Caching

2) **les fournisseurs d'accès à Internet (5 FAI en Nouvelle-Calédonie) assurant aussi des opérations de « caching »,**
3) **et les hébergeurs (FAI, agences de communications, webdéveloppeurs, CITIUS, DSP, etc.)**.

S'agissant des opérateurs de communications électroniques, compte tenu de leur fonction purement technique, et ne disposant d'aucun moyen pour apprécier le contenu des messages transférés, leur responsabilité ne peut être retenue.

Ainsi dans son article 9, la LCEN définit l'opérateur comme « *toute personne assurant une activité de transmission de contenus sur un réseau de télécommunications* ».

Il organise la responsabilité du « *simple transport* », autrement dit la fourniture d'un service de la société de l'information consistant à transmettre, sur un réseau de communication, des informations fournies par le destinataire du service.

Quant aux opérateurs assurant une activité de « caching », le même article 9 les définit comme « *toute personne assurant dans le seul but de rendre plus efficace leur transmission ultérieure, une activité de stockage automatique, intermédiaire et temporaire des contenus qu'un prestataire transmet* ».

Ces deux définitions ont été codifiées aux articles L. 32-3-3 et L. 32-3-4 du code des postes et télécommunications, articles applicables à la Nouvelle-Calédonie.

Enfin, le fournisseur d'hébergement est un fournisseur de services (service provider). Il dispose sur son serveur d'un espace qu'il cède à un éditeur pour que ce dernier puisse «héberger» son site, le plus souvent contre rémunération. L'article 6-I.2 de la LCEN, définit les fournisseurs d'hébergement comme les « *personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services* ».

Le fournisseur d'accès peut mettre à la disposition de l'utilisateur un espace sur son serveur pour «héberger» un site webA ce titre, il joue à la fois le rôle de fournisseur d'accès à Internet et d'hébergeur. Ce qui est le cas parmi les cinq FAI en Nouvelle-Calédonie.

B- L'opérateur numérique, interprète de la notion d'informations illicites

Premier point à mettre en exergue au regard de la lecture de la LCEN :

Les FAI et fournisseurs d'hébergement ne sont pas soumis à une obligation générale de surveiller les informations qu'elles transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites.

Toutefois, s'agissant de l'hébergeur, les articles 6-1.2 et suivants disposent qu'il peut engager sa responsabilité civile ou pénale du fait des activités ou des informations stockées lorsqu'il a eu connaissance de leur caractère illicite ou lorsqu'il n'a pas agi promptement pour retirer ces données, ou en rendre l'accès impossible.

Par ailleurs, si les contenus ont été créés par des personnes agissant sous l'autorité ou le contrôle de l'hébergeur, il est évident que ce dernier engage aussi sa responsabilité. Car, dans cette hypothèse, son intervention perd un caractère purement technique.

Enfin, lorsqu'un hébergeur intervient une première fois pour supprimer un contenu manifestement illicite, il doit ensuite mettre tout en œuvre pour que ce contenu ne fasse pas à nouveau l'objet d'une nouvelle publication sur son site. Dans le cas contraire, le juge serait plus sévère à son égard, au regard du précédent.

ZOOM

Le 15 novembre 2004, le Tribunal de Grande Instance a rendu la première décision sur la responsabilité d'un hébergeur en application de la LCEN.

En l'espèce, le Comité de défense de la cause arménienne (CDCA) assigne, le 9 juillet 2004, le Consul Général de Turquie à Paris ainsi que la société Wanadoo France Télécom, hébergeur du site Internet du consul. Le comité avait constaté sur des sites Internet hébergés en France dans les pages personnelles de Wanadoo, la mise en ligne d'un pamphlet à vocation clairement négationniste contestant le génocide arménien.

Le juge a considéré que la négation du génocide arménien ne constituait pas une violation manifeste du principe de la dignité de la personne humaine au regard des dispositions de la loi du 21 juin 2004.
Pour juger de la responsabilité de Wanadoo, le juge s'est référé explicitement à la LCEN et bien que sa décision soit favorable à l'hébergeur, **l'interprétation de la notion de contenu « manifestement illicite » reste floue.**

En donnant un trop grand pouvoir d'interprétation à la notion de « contenus illicites » à l'hébergeur, cela risque d'aboutir à une censure en amont du Net par le prestataire technique.

En d'autres termes, ce dernier préfèrerait avoir une vision large de ce qui est 'illicite', plutôt que de courir le risque d'une condamnation par le juge.

De manière plus simple, il faut interpréter la notion 'illicite' de l'article 6 de la LCEN 'in concreto', c'est à dire en fonction des connaissances juridiques que l'on peut attendre d'un hébergeur. [2]

[2] Avis de Lionel Thoumyre, alors chargé de mission pour le Forum des droits sur l'Internet

C- L'opérateur numérique, relais des autorités judiciaires

Considérés comme *« les personnes dont l'activité est d'offrir un accès à des services communication au public en ligne »,* les fournisseurs d'accès n'exercent qu'un rôle technique, en permettant au public d'accéder aux services de l'internet, assurant ainsi la mise en relation du public avec les services de communication en ligne.

Cependant, au nom de la lutte contre les infractions réalisées sur Internet, la loi LCEN met à la charge du fournisseur d'accès un certain nombre d'**obligations** qui d'une part, vont permettre d'identifier l'auteur de l'infraction afin de le poursuivre et d'autre part, de lutter directement contre l'infraction.

L'obligation de **conservation des données** d'identification désormais imposée au fournisseur d'accès vient se substituer au principe initial d'effacement des données de communication.

Certes, ce principe prévoyait déjà quelques exceptions, notamment : « *Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire d'informations, il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques. »*
Mais l'article 6-II de la LCEN fait, de cette exception, une obligation générale pour les FAI afin d'assurer la transparence des activités menées par ses clients et de permettre l'identification des éditeurs de services.

La loi n°2006-64 du 23 janvier 2006 relative à la **lutte contre le terrorisme** prévoit en outre que *« les agents individuellement désignés et dûment habilités des services de police et de gendarmerie»* peuvent obtenir certaines données de la part des opérateurs techniques et ce, sans autorisation judiciaire préalable.

Cette obligation vise les « *personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion».* Elle ne concerne donc que les FAI et les opérateurs de téléphonie (ex : OPT en Nouvelle-Calédonie). Les hébergeurs sont exclus.

Le Conseil d'Etat, a estimé que cette obligation, amplement critiquée par les FAI, ne porte pas une atteinte disproportionnée au respect de la vie privée par rapport aux buts de sécurité publique.
D'autant plus que cette obligation de conservation se doublait d'une obligation de communication exclusive aux autorités judiciaires.

Les FAI sont donc de plus en plus sollicités pour lutter directement contre les infractions.
-Ils sont ainsi astreints à mettre en place un **dispositif de signalement de contenus odieux** relatifs aux crimes de guerre, crimes contre l'humanité, provocation à la discrimination, à la haine ou à la violence raciale. En corollaire, ils doivent informer promptement les autorités publiques compétentes et **rendre publics les moyens consacrés à la lutte contre ces activités illicites**.
-Ils doivent obtempérer à une **demande judiciaire** de « *surveillance ciblée et temporaire* », notamment pour **bloquer l'accès à un site illicite** ou encore pour identifier un de leurs abonnés (article 6-I.8 LCEN)[3].

Comme les FAI, les hébergeurs sont soumis à l'obligation **d'identification et de communication des auteurs de l'infraction** et doivent à ce titre **détenir et conserver les données** permettant d'identifier l'auteur.
Ils peuvent également être sanctionnés au nom de leur obligation de conservation de données d'identification crédibles, lorsque les données présentent un caractère manifestement fantaisiste, empêchant ainsi l'identification de l'auteur.

Il ressort de l'ensemble de ces éléments que peu à peu, le législateur et le juge ont multiplié le nombre d'obligations incombant à l'hébergeur et plus encore au FAI.
Ces prestataires font face à des problèmes techniques délicats et dans le même temps voient leur responsabilité juridique accrue, ce qui les entraîne vers des contrôles plus poussés. Cela se traduit finalement par une atteinte ouverte aux libertés des internautes.

L'opérateur numérique :
Responsable de traitement au sens de la loi informatique et Libertés (CNIL)

De cette loi, l'opérateur doit ressortir trois types de vigilance, à l'égard de :
- ses clients,
- la CNIL,
- ses partenaires économiques.

Au sens de l'article 3 de la loi informatique et libertés, le **responsable de traitement** est « *la personne, l'autorité publique, le service ou l'organisme qui détermine la finalité et les moyens du traitement*[4] *mis en œuvre* ».
« Le rôle premier de la notion de responsable du traitement est de déterminer qui est chargé de faire respecter les règles de protection des données, et comment les personnes concernées peuvent exercer leurs droits dans la pratique. ***En d'autres termes, il s'agit d'attribuer les responsabilités.*** *»*[5]

[3] Ainsi le juge peut exiger la mise en place de filtres empêchant le transfert par Peer to Peer de fichiers musicaux portant atteinte au droit d'auteur, sans que cela crée, pour les FAI, une obligation générale de surveillance.

[4] Traitement (de données à caractère personnel) : « Opérations relatives à la collecte, l'enregistrement, l'élaboration, la modification, la conservation et la destruction d'informations nominatives ainsi que tout ensemble d'opérations de même nature se rapportant à l'exploitation de fichiers ou bases de données et notamment les interconnexions ou rapprochements, consultations ou communications d'informations nominatives ». (article 2 loi Informatique et Libertés)

[5] Extrait de l'avis du groupe 29 de 2010 sur les notions de responsables de traitement et sous-traitant

On peut en outre affirmer que la détermination des finalités et des moyens revient à établir respectivement le «pourquoi» et le «comment» de certaines activités de traitement.

A- Droits de l'abonné à la téléphonie dans l'utilisation de ses données personnelles

La définition d'une donnée à caractère personnelle[6] est très large. Celle-ci permet d'identifier directement ou indirectement un individu (par ex : son nom, sa date de naissance, son adresse électronique, ses coordonnées bancaires).

L'abonné d'un opérateur dispose en vertu de la loi informatique et libertés de droits lui permettant de contrôler l'utilisation de ses informations personnelles.

En Nouvelle-Calédonie, cela concerne l'OPT qui est l'unique opérateur de téléphonie fixe et mobile.

1. Le droit à l'information (article 32 LIL)

L'opérateur doit informer l'usager :

- de l'utilisation qui sera faite de ses données ;
- du caractère obligatoire ou non de ses réponses ;
- des destinataires de ces données ;
- de leur transfert éventuel hors de l'Union européenne (par exemple vers des centres d'appels) ; cette exigence en Nouvelle-Calédonie peut se concevoir par exemple en cas de transfert vers l'Australie ou la Nouvelle-Zélande. (Voir Supra).
- des droits dont il dispose (droits d'opposition, d'accès et de rectification).

Cette information doit être portée à sa connaissance sur le contrat ou dans les conditions générales de service.

[6] Article 2 loi CNIL : « Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. »

2. Le droit d'opposition (article 38)

L'usager peut s'opposer à ce que des données le concernant soient enregistrées dans les fichiers de l'opérateur, sous réserve d'avancer des raisons légitimes. Cette condition des 'raisons légitimes n'existent plus en cas de prospection commerciale.

C'est à l'opérateur d'apprécier les suites à apporter à la demande. En cas de désaccord, la justice peut être saisie.

En revanche, l'usager peut s'opposer à ce que son opérateur lui adresse des propositions commerciales ou qu'il transmette ses données à des partenaires commerciaux.

Afin que l'usager puisse facilement exercer ce droit, la CNIL recommande qu'une case à cocher soit apposée sur les formulaires de collecte des données.

3. Le droit d'accès (article 39)

C'est le droit d'obtenir, sous une forme compréhensible, une copie des informations concernant le client et enregistrées dans les fichiers de l'opérateur ou de ses partenaires commerciaux.

Ce droit peut s'exercer sur place ou par écrit en justifiant de son identité (copie d'une pièce d'identité).

B- L'obligation d'alerte des opérateurs numériques à la CNIL : la faille de sécurité

L'article 34 bis de la Loi informatique et libertés a introduit la notion de **faille de sécurité** (ou violation de données à caractère personnel) dans la législation française.

Cette disposition est également applicable en Nouvelle-Calédonie.

Il s'agit de toute violation de la sécurité entrainant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données à caractère personnel faisant l'objet d'un traitement dans le cadre de la fourniture au public de services de communications électroniques.

En cas de violation, les opérateurs d'accès et de services de communications électroniques accessibles au public doivent avertir la CNIL. Lorsque cette violation peut porter atteinte aux données personnelles ou à la vie privée d'un abonné ou d'une autre personne physique, le FAI informe également sans délai l'intéressé.

Cette notification n'est toutefois pas nécessaire si la CNIL a constaté que des mesures de protection appropriées ont été mises en œuvre par les opérateurs numériques afin de rendre les données incompréhensibles à toute personne non autorisée à y avoir accès.

ZOOM

A titre, d'exemple, en avril 2014, une faille de sécurité, dénommée « Heartbleed », a été découverte dans certaines versions du logiciel OpenSSL sur lequel s'appuie une grande partie de la sécurité du Web.
Tout opérateur mettant en œuvre une version vulnérable d'OpenSSL aurait dû en vertu de l'article 34-II de la loi informatique et libertés :
- mettre à jour les serveurs vulnérables, afin de ne plus utiliser de version affectée par la faille ;
- révoquer les clés et certificats utilisés ;
- renouveler les clés et mettre à jour les certificats correspondants ;
- conseiller aux utilisateurs de renouveler leurs moyens d'authentification, notamment leurs mots de passe.

Chaque fournisseur de services de communications électroniques doit à ce titre tenir à jour un inventaire des violations de données personnelles, notamment de leurs modalités, de leur effet et des mesures prises pour y remédier et conserver cet inventaire à la disposition de la CNIL (art. 34-III loi Informatique et libertés).

C- les opérateurs numériques et ses relations commerciales

1-Transfert de données personnelles vers un partenaire local

Lorsqu'un FAI par exemple souhaite communiquer des données à caractère personnel à l'un de ses partenaires, il doit obligatoirement recueillir au préalable le consentement express de l'usager. Nous ne sommes plus ici dans le champ du simple devoir d'information étudié précédemment, mais dans un **véritable recueil de l'accord de l'usager**. Ce principe est appelé 'opt-in' ; il prend le plus souvent la forme d'une case à cocher qui s'exprime sous la forme suivante :

Si vous ne souhaitez pas que vos coordonnées soient transmises à nos partenaires commerciaux, cochez :

☐ *cette case*

Un fichier de clients utilisé à des fins de prospection peut faire l'objet d'une déclaration de conformité à la norme n°48 (déclaration simplifiée). Les dispositifs qui n'entrent pas dans le cadre de cette norme doivent faire l'objet pour leur part, d'une déclaration normale auprès de la CNIL.

2- Transfert de données personnelles vers un pays situé hors de l'union européenne

Il y a transfert de données hors UE, lorsque les données à caractère personnel sont transférées depuis le territoire européen vers un ou des pays situés hors de l'Union européenne. Le transfert peut s'effectuer, par copie, par déplacement de données, par l'intermédiaire d'un réseau ou d'un support à un autre (exemple d'un disque dur à un serveur).
Ainsi, l'envoi de données à caractère personnel par courrier électronique, l'hébergement de données ou encore les accès à une base de données à distance sont considérés comme des transferts de données à caractère personnel.

Un prestataire technique doit disposer d'une vigilance accrue en cas de transfert de données dans un pays n'appartement pas à l'Union Européenne et considéré par la CNIL comme n'offrant pas un niveau de protection adéquat ou suffisant.

En effet, ces transferts sont en principe interdits, sauf dans les cas suivants :
-la mise en place de clauses contractuelles ou de règles internes d'entreprises. Dans ce cas, une autorisation de la CNIL s'avère toutefois toujours nécessaire ;
-pour les exceptions prévues par l'article 7 de la loi informatique et libertés (ex : en cas de consentement de la personne concernée par les données, lorsque le transfert est nécessaire à la sauvegarde de la vie de la personne…).

Dans le cadre spécifique à la Nouvelle-Calédonie, une vigilance sera requise en cas de transfert vers le Vanuatu ou le Japon. Ces pays ne disposent pas en effet d'un niveau de protection des données personnelles suffisant pour la CNIL.
En revanche, l'Australie et la Nouvelle-Zélande sont considérées par l'Union européenne comme des pays offrant un cadre sécurisé. L'autorisation préalable de la CNIL ne sera donc pas requise pour eux.

3- le recours à la sous-traitance par les opérateurs numériques

Lorsqu'un responsable de traitement, ce qu'est en l'occurrence un fournisseur de communications électroniques, souhaite recourir à un sous-traitant, il doit s'assurer que ce dernier présente des garanties suffisantes pour mettre en œuvre des mesures de sécurité et de confidentialité de données personnelles.

Un contrat doit être conclu avec son sous-traitant indiquant :
-que le sous-traitant a l'obligation d'agir selon les instructions du responsable de traitement,
-les obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données (art. 35 loi Informatique et libertés).

Le sous-traitant devra à titre d'exemple s'engager :
-à la non divulgation de données personnelles à l'extérieur,
-prendre les mesures de nature à éviter toute utilisation détournée ou frauduleuse des données précitées,
-effectuer des mesures de sauvegarde régulière ou mettre en œuvre des procédures de gestion des incidents.

Toutefois, l'opérateur numérique de traitement restera toujours responsable de la gestion et de la protection des données confiées à son sous-traitant. Pour cela, il est fortement souhaitable qu'il prévoit des audits réguliers auprès de ses sous-traitants.

Sources

www.cnil.fr
-Guide 'téléphonie' de la CNIL
-CNIL-Guide_securite_avance_Mesures
-CNIL-Guide_Securite_avance_Methode
-Délibération n°2007-391 du 20 décembre 2007 portant avis de la CNIL sur le projet de décret pris pour l'application de l'article 6 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, et relatif à la conservation des données de nature à permettre l'identification de toute personne physique ou morale ayant contribué à la création d'un contenu mis en ligne
« La responsabilité extracontractuelle des fournisseurs d'accès à Internet » Ouvrage de Willy Duhen.
« La responsabilité des acteurs de l'Internet » de Oriane Ibanez. Mémoire IREDIC.
La responsabilité des fournisseurs d'accès et d'hébergement. Article de PHILIPPE GILLIÉRON.