PETIT GUIDE JURIDIQUE A L'USAGE DES ASSOCIATIONS D'INFORMATIQUE ET RÉSEAU

-

Corentin ‘eugene’ Pane

corentin.pane[at]gmail.com

-

28 mars 2016

-

Édité par FedeRez
Federez.net

Table des matières

Introduction

Vous faites partie ou vous dirigez une association qui maintient un réseau ? Qui fournit un accès Internet à ses membres ? Qui possède une infrastructure WiFi ? Qui propose des services d'hébergement Web ou de fichiers, un annuaire, des bases de données, des emails ? Si la réponse à l'une de ces questions est oui, alors ce guide est fait pour vous !

Pourquoi lire ce guide ?

En France, toute association constitue une personne morale, avec des droits, des devoirs, un domicile... et des responsabilités. Et ces responsabilités sont souvent reportées sur les personnes bien physiques que sont les dirigeants de l'association et notamment son Président et son Trésorier. Ainsi les dirigeants peuvent être reconnus responsables et se retrouver condamnés par un tribunal pour des actions commises par d'autres membres de l'association. Sans pour autant sombrer dans un peur irraisonnée, il est nécessaire de bien connaitre ses droits et devoirs en tant que dirigeant d'une association. D'autant plus que vos associations ont des activités bien particulières que sont les activités dites de "communications électroniques" et de "services électroniques", et qu'il y a de nombreux pièges à éviter.

L'objectif de ce guide est de donner à vos associations d'informatique et réseau (tels que les membres de FedeRez) les clefs et outils nécessaires à la compréhension et à l'exercice de vos droits et devoirs.

Pourquoi croire ce qu'il y a écrit dedans ?

Ce guide a été rédigé par des anciens dirigeants d'association réseau et membres du bureau de FedeRez, qui ont eu plus d'un problème en lien avec le droit... Tout ce qui est écrit dans ce guide est annoté par le cadre légal et réglementaire correspondant : nous irons croiser le code des postes et des communications électroniques, la loi informatique et liberté, la loi pour la confiance dans l'économie numérique, les règlements européens, le code civil, le code pénal, les jurisprudences diverses et variées et même le code de la défense et le code de la sécurité intérieure... Nous avons tout épluché pour vous ! Bonne lecture !

I L'activité de FAI

a) Le statut de FAI, de fait ou de droit

Qu'est-ce qu'un opérateur ? Quelle différence avec un FAI (fournisseur d'accès Internet) ? Quel rapport avec les FAI comme Orange, Free ou SFR ? Commençons par quelques définitions[1] :

Opérateur : on entend par opérateur toute personne physique ou morale exploitant un réseau de communications électroniques ouvert au public ou fournissant au public un service de communications électroniques.

Communications électroniques : on entend par communications électroniques les émissions, transmissions ou réception de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique. Donc tout ce qui passe sur un câble, une fibre, par les ondes...

FAI : un FAI est un opérateur qui propose à des abonnés un accès à Internet. L'accès à Internet est en effet un service de communications électroniques ! Dans la suite, nous parlerons de FAI même si votre association ne fournit pas d'accès Internet à proprement parler et fournit uniquement un réseau local (LAN). Il faut savoir que les droits et devoirs sont identiques sur *tous* les réseaux, qu'ils soient connectés à Internet ou non !

Si votre association propose à ses membres un accès réseau ou Internet, vous êtes donc un FAI comme Orange et Free, mais à plus petite échelle. Et vous devez vous déclarer comme tel auprès de l'ARCEP.

b) L'ARCEP

L'ARCEP est l'Autorité de Régulation des Communications Électroniques et des Postes. Ses moyens et compétences sont précisés dans le Code des postes et des communications électroniques[2]. L'ARCEP est une autorité indépendante qui régule les réseaux de communication en France : elle s'assure de la qualité de service, de la libre concurrence, de l'attribution des fréquences radioélectriques... et de manière générale du respect des opérateurs de leurs obligations. Elle a d'ailleurs le pouvoir de sanctionner les opérateurs contrevenants (même si en pratique seuls les grands FAI nationaux sont visés).

Il est obligatoire sous certaines conditions de déclarer votre association à l'ARCEP[3]. Cela vous confère des droits supplémentaires et vous permet d'exercer votre activité en vous exonérant de tout un tas de responsabilités. N'hésitez pas à consulter leur site et à lire leur guide juridique ![4]

Plus de 1200 opérateurs sont déclarés à l'ARCEP, dont un quelques-uns sont à FedeRez ! Voir en annexe pour réaliser sa déclaration auprès de l'ARCEP.

Il vous est conseillé de prendre en compte la déclaration à l'ARCEP dans vos statuts, vous trouverez en annexe des exemples d'articles à ajouter.

[1] Tirées de l'article L32 15° du Code des postes et des communications électroniques (CPCE)
[2] Articles L32, L32-1 et suivants du CPCE
[3] Articles L32-1 I 1° et L33-1 du CPCE
[4] http://arcep.fr/uploads/tx_gspublication/guide-juridique-crip2007.pdf

c) Responsabilité des opérateurs

On entend souvent dire : "En tant que FAI, vous avez le devoir de surveiller ce que font vos abonnés, il faut s'assurer qu'ils ne commettent pas d'infraction sinon vous en êtes responsables. D'ailleurs vous êtes responsables, mais le gestionnaire de la résidence aussi, et même le directeur de votre école peut aller en prison". Désormais, vous savez que tout ceci est faux ! Bien au contraire, sachez que vos utilisateurs sont entièrement responsables de leurs activités sur le Net et que chercher à les protéger vous expose à des poursuites dans de nombreux cas...

La loi est claire : votre responsabilité n'est jamais engagée à raison des contenus échangés sur votre réseau, que ce soit entre les utilisateurs en local ou vers l'extérieur[5]. Ceci étant dit, nous reviendrons plus en détail sur pourquoi vous n'avez pas le droit d'empêcher vos utilisateurs de faire ce qu'ils veulent en partie II.

d) Obligations des FAI : logs, réseaux WiFi et hertziens et authentification

En tant que FAI, votre association a un certain nombre d'obligations.

Vous sauvegardez peut-être en base de donnée les fameux "logs" : souvent ce sont des logs DHCP ou des logs radius qui permettent d'effectuer la correspondance entre un utilisateur et son adresse sur le réseau (adresse IP, avec un port si vous faîtes du NAT) à une heure donnée. Si vous ne les sauvegardez pas, il faut immédiatement commencer à le faire ! **C'est une obligation pour les opérateurs de conserver ces données pendant une durée d'un an exactement[6]**. A quoi servent-elles ? Elles serviront à identifier le coupable d'une infraction sur votre réseau. Mais patience, car l'accès à ses données est extrêmement réglementé et vous-mêmes n'avez pas le droit d'y accéder sans autorisation exceptionnelle (vous vous exposez à des poursuites dans le cas contraire ![7]) que nous verrons plus en détail en partie II. Attention cependant : **les données que vous conservez ne peuvent en aucun cas concerner le contenu des communications électroniques[8] donc aucune URL, aucun header HTTP, aucun historique**. Dans le cas contraire, vous êtes en plein dans l'atteinte à la vie privée des personnes et vous risquez, encore une fois, gros[9]. Il ne faut sauvegarder que les données permettant, à partir d'un *timestamp* et d'une adresse IP donnée, de retrouver l'utilisateur correspondant. Pas plus, pas moins ! Vous avez également un devoir de protection de ces données : vérifiez qu'elles sont bien répliquées car vous risquez beaucoup en cas de perte accidentelle.

Vous devez donc mettre en place, si ce n'est pas déjà fait, un moyen d'authentifier les utilisateurs pour être en mesure de déterminer, à toute heure, quel individu se cache derrière telle adresse IP (et tel port en cas de NAT). L'authentification par radius couplée à du WPA2 Entreprise pour du WiFi est une solution largement adoptée à travers le monde. Et encore un rappel : **même votre association n'a pas le droit d'aller consulter ces logs d'authentification !**

[5] Article L32-3-3 du CPCE
[6] Article L34-1 III du CPCE
[7] Article 226-22 du Code pénal, article 226-21 du Code pénal et article L34-1 III du CPCE
[8] Article L34-1 VI du CPCE
[9] Article 9 code civil, articles 226-1 et 226-15 du Code pénal

Concernant les ondes désormais : si vous mettez en place un réseau WiFi ou hertzien (avec des antennes), il faut faire attention à deux choses :

- la puissance d'émission qui est très réglementée en France[10] avec 100mW au maximum pour la bande 2.4Ghz ;
- et les bandes de fréquences que vous utilisez. En effet, seules les bandes 2.4Ghz et 5GHz sont libres et ne requièrent pas d'autorisation particulière pour les exploiter (réseaux WiFi, bridges WiFi, antennes directionnelles...). Pour utiliser des fréquences en dehors de ces bandes, renseignez-vous auprès de l'ARCEP ou de l'Agence nationale des fréquences[11].

En conclusion : vous vous déclarez à l'ARCEP, vous sauvegardez pendant un an des données *limitées* d'identification des utilisateurs, vous ne consultez pas ces données et ne les divulguez à personne (ou presque, voir partie II pour plus de détails) ; et vous n'utilisez que les fréquences radioélectriques autorisées.

e) Cas des DSI et de RENATER

Si vous possédez votre propre lien vers l'Internet mondial, vous faites partie des exceptions chez les associations étudiantes.

Dans bien des cas, c'est la DSI de votre école (aussi appelée CRI, CTI, DRI…) qui vous fournit gracieusement un accès à Internet grâce à son abonnement à RENATER. Et bien que votre DSI le sache ou non, qu'elle l'accepte ou non, elle est également opérateur ! Alors certes elle ne va pas se déclarer à l'ARCEP car ce n'est pas son rôle premier et elle se mettrait dans une situation difficile vis-à-vis de RENATER: RENATER interdit aux établissements de reverser une partie de la connexion à des sites tiers, incluant les résidences étudiantes. Et oui, votre DSI peut parfois vous imposer des limitations mais sachez qu'elle brave l'interdit de la charte RENATER pour cela[12].

A y regarder de plus près, les conditions imposées par RENATER et votre DSI sont assez restrictives et semblent s'opposer à un principe qui peut ou non vous être familier : la neutralité de l'Internet. RENATER impose une utilisation à des fins d'enseignement, de pédagogie et de recherche à ses utilisateurs, et par-dessus cela votre DSI, souvent, vous place derrière un pare-feu sévère et vous bloque l'accès au p2p, aux jeux en ligne, aux sites à caractère pornographiques, au streaming vidéo... **Et bien c'est cela, une atteinte à la neutralité de l'Internet : lorsqu'une discrimination du trafic est effectuée, que tous les flux ne sont pas égaux entre eux et que des blocages sont appliqués**. Comme quand certains opérateurs font payer plus cher pour plus de débit. Devinez quoi, **c'est illégal !**[13][14]

Que pouvez-vous faire concrètement ? Malheureusement, vous êtes dans une situation où vous n'avez pas les moyens de négocier grand-chose... Comptez sur votre charisme naturel pour convaincre votre DSI de rouvrir le *torrent* sur votre réseau. Ou lors, envisagez de sortir du carcan de RENATER...

[10] http://www.arcep.fr/index.php?id=9272
[11] http://www.anfr.fr
[12] https://www.renater.fr/IMG/pdf/charte_fr.pdf
[13] Article 11 du projet de loi pour une République Numérique
[14] Arrêt de la CJUE, 24 novembre 2011, SABAM C/ Scarlet Extended

f) Franchir le pas pour sortir de RENATER

Sortir de la dépendance vis-à-vis de votre école et DSI, et donc de RENATER, peut être une solution à ces problèmes de débit ou de conditions d'accès. Il faut se renseigner auprès des préfectures pour savoir si une fibre privée ne passe pas loin de vos résidences, se renseigner auprès des opérateurs si leurs offres professionnelles vous conviennent, voir avec votre gestionnaire de résidence pour d'éventuels travaux... Il faut savoir qu'un transit de 1Gbps coûte auprès d'un opérateur privé entre 1000€ et 2000€ par mois selon les conditions techniques du débit et des garanties voulues, et que des travaux pour poser une fibre peuvent coûter quelques centaines de milliers d'euros. Il faudra peut-être serrer la ceinture ou augmenter les cotisations !

II Les infractions commises sur vos réseaux par vos adhérents

Nous verrons ici les infractions communes commises par beaucoup de gens sur Internet, les choses à faire et ne pas faire en termes de régulation et de filtrage, et la réaction appropriée à avoir en cas de requête judiciaire ou administrative.

a) Liste des infractions volontaires ou non

Vos adhérents ou abonnés commettent un nombre incalculable d'infractions sur les réseaux, sans forcément le savoir. En voici une petite liste non exhaustive :

- Téléchargement, téléversement, mise à disposition, possession, copie, stockage, consultation... de contenus illicites : à chaque fois que vous regardez un *stream* gratuitement ou que vous téléchargez en *torrent* le dernier blockbuster hollywoodien.

- Diffamation et injure, même en blaguant, sur les réseaux sociaux ou un forum.

- Atteinte au copyright lorsque vous détournez sur Photoshop une œuvre protégée.

- Utilisation illicite de logiciels sous licence *crackés*.

- Atteinte à la vie privée lorsque vous dévoilez des informations sensibles sur une personne ou un groupe.

- Usurpation d'identité lorsque vous profitez d'un compte Facebook malencontreusement laissé ouvert sur l'ordinateur d'un ami.

- Collecte illicite d'informations personnelles lorsque vous récoltez des informations sensibles auprès de nombreuses personnes, même dans le cadre associatif ou d'un travail scolaire.

- Spam, lorsque vous … spammez et concourrez à la diffusion d'une menace de *phishing*.

- et la liste ne s'arrête pas là ! Toutes les infractions punies par la loi ou presque peuvent se transposer en ligne.

b) Quelle régulation est possible ?

Grande question, courte réponse : très peu de choses de votre propre initiative. En fait, à part faire signer une charte de bon comportement à vos abonnés, vous ne pouvez rien faire ! Et si certaines conditions sont souvent imposées par votre DSI sous prétexte de RENATER, sachez que c'est illégal. Vous pourrez trouver en annexe un dossier juridique sur lequel appuyer votre argumentation en cas de besoin.

En effet, le filtrage avec un pare-feu des communications pour bloquer le p2p ou tout autre flux est interdit par la loi, pour de nombreuses raisons : c'est d'abord une atteinte à la vie privée des adhérents ! Ensuite, il est interdit de prendre frauduleusement connaissance des correspondances électroniques émises sur un réseau[15] : c'est exactement ce qui est fait lorsqu'un pare-feu décide ou non de bloquer ou non un flux... Ça vous dit quelque chose, les « boîtes noires » du gouvernement ?

[15] Articles 226-1 et 225-15 du Code pénal

La seule exception : lorsqu'un juge ou la direction générale de la police nationale vous le demande[16] ! A ce moment-là seulement, vous avez le devoir de procéder selon les conditions qu'ils vous imposent au blocage desdits sites Internet. **Votre DSI n'est absolument pas habilitée à vous imposer ou faire imposer un filtrage**, d'ailleurs la Cour de Justice de l'Union Européenne confirme que bloquer le p2p sur un réseau est illégal[17].

Qu'est-ce qu'on peut faire alors ? Rien du tout de concret, mais **il est tout de même conseillé de faire signer à vos adhérents une charte de bon comportement sur votre réseau**, qui leur rappelle le cadre légal et réglementaire et leur précise les principales infractions qu'ils pourraient commettre. De cette manière, vous prouvez votre bonne foi. Vous trouverez en annexe un exemple d'une telle charte, qui peut être individuellement signée par les adhérents ou bien annexée au formulaire d'adhésion ou dans votre Règlement Intérieur.

c) Réagir aux plaintes des ayants-droits

A part le désormais fameux "prétexte RENATER " présenté par les DSI, vous avez peut-être entendu parler des **ayants droits**.

Un ayant droit est une personne physique ou morale détenant un droit du fait de son lien avec l'auteur, dans le cadre du copyright. Les sociétés d'ayant droit surveillent le Web à la recherche de contenus illicites protégés par droit d'auteur et mettent en place des techniques pour déceler les téléchargements illégaux. Elles envoient régulièrement des alertes par email aux responsables informatiques concernant l'adresse IP suspectée d'avoir téléchargé illégalement un fichier protégé par droit d'auteur, pour demander à ce que cela cesse, voire demander une réparation financière et peut-être même une demande d'identification de la personne concernée.

Lorsque vous recevez un tel avertissement, directement ou suite à un *forward* de votre DSI, une seule chose à faire : **déplacer le message vers la corbeille sans y répondre**. Et oui ! La dernière chose à faire et d'y répondre et encore moins de dénoncer la personne qui se cachait derrière l'adresse IP annoncée. **Rappel : seules les autorités compétentes nationales peuvent vous demander d'accéder à des données relatives au trafic de vos abonnés** (voir détail dans en *d)* et *e)*) et fournir des informations à un tiers non autorisé vous expose sérieusement à des poursuites pénales, pour violation de données à caractère personnel, utilisation illicite de fichiers de base de donnée et atteinte à la vie privée.

Le seul moyen pour qu'un ayant droit obtienne réparation, c'est qu'il porte plainte contre X pour téléchargement illégal et qu'un juge se tourne ensuite vers vous avec une requête judiciaire vous demandent d'identifier la personne (voir *e)*)...

[16] Article 6-1 de la Loi pour la confiance dans l'économie numérique (LCEN) et le décret n° 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique
[17] Arrêt de la CJUE, 24 novembre 2011, SABAM C/ Scarlet Extended

d) Réagir aux requêtes administratives

Vous pourrez recevoir, exceptionnellement, des demandes de la part d'autorités administratives compétentes[18]. Qui peut vous demander quoi ? La Hadopi, l'ANSSI, la gendarmerie nationale et la police nationale sont habilitées à vous demander l'accès aux *logs* que vous sauvegardez, les fameux *logs* que vous devez conserver un an. A ces gens-là seulement, et dans les conditions qu'ils détaillent, vous devez transmettre les informations personnelles qu'ils vous demandent et dont vous disposez : n'en donnez pas plus ! Bien souvent, ils vous demanderont simplement d'identifier qui utilisait telle adresse IP à telle heure...

Il peut arriver que la direction générale de la police nationale (office central de lutte contre la criminalité liée aux TIC) vous demande de mettre en place un blocage[19] d'un certain nombre de sites à caractère pédopornographique ou d'incitation terroriste. Vous recevrez directement et confidentiellement une liste de sites à bloquer et les types de blocage à mettre en œuvre. Vous n'êtes sinon, de manière générale, soumis à aucune obligation de surveillance ou de recherche de contenus illicites[20]. Attendez que la police vous le demande !

De manière encore plus exceptionnelle, vous pourrez recevoir une demande de la part d'un service de renseignement spécialisé avec autorisation du Premier ministre de mettre en place un dispositif d'écoute sur votre réseau pendant une durée de 48h pour les besoins de défense nationale et prévention du terrorisme et de la criminalité organisée. Les personnes habilitées à vous faire une telle demande sont la DGSI, la DGSE, la direction de la protection et de la sécurité de la défense, la direction du renseignement militaire, la direction nationale du renseignement et des enquêtes douanière et le service de traitement du renseignement et action contre les circuits financiers clandestins[21].

En dehors de ces administrations-là, ne communiquez rien à personne (même pas à vous-mêmes) !

e) Requêtes judiciaires

Le dernier cas de demande légitime que vous pourrez recevoir, est le cas de la requête judiciaire. **Un juge d'instruction, un magistrat ou le Procureur de la République peut, dans le cadre d'une enquête, vous demander n'importe quelle information dont ils peuvent avoir besoin, y compris vous demander de mettre en place un dispositif d'écoute à l'insu de quelqu'un. Un juge peut enfin vous demander de bloquer l'accès à un site Internet**.[22] Vérifiez bien le mandat fourni et renseignez-vous auprès d'un avocat ou juriste pour être sûr de ne pas faire de bêtises, mais les délais indiqués sont courts, avec souvent 24h pour procéder aux blocages.

Et rassurez-vous : ce genre de requêtes se produit très rarement ! Le plus souvent, ce sont des requêtes illégitimes d'ayants droits qui envoient quelques messages par an et qui terminent à la poubelle...

[18] Article L34-1 III du CPCE
[19] Article 6-1 de la LCEN et le décret n° 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique
[20] Article 6 7° de la LCEN
[21] Décret n° 2015-1185 du 28 septembre 2015 portant désignation des services spécialisés de renseignement
[22] Articles 77-1-1 et 706-102-1 du Code de procédure pénale

III Les autres activités numériques et d'informatique

Dans la vie de votre association, il n'y a peut-être pas que l'accès à Internet ou à un réseau ! En effet, vous proposez de nombreux services à vos adhérents. Voilà les différents pièges à éviter et les indications pour se conformer au droit.

a) Hébergement de contenus

Un hébergement de contenu regroupe les hébergements de sites Web, les hébergements de fichiers de type *owncloud*[23], les FTP (publics ou privés), les SAN, les NAS... Finalement, tout support connecté au réseau sur lesquels des membres peuvent lire ou écrire du contenu.

Dans ce cas, encore une fois, vous n'avez pas de souci à vous faire : **votre responsabilité ne peut être engagée à raison des contenus illicites stockés si vous n'en aviez pas connaissance ou si vous les avez promptement retirés lorsque vous en avez pris connaissance**[24]. Vous avez une obligation cependant : permettre d'identifier l'auteur d'un contenu ou le responsable de la publication de tout contenu que vous hébergez[25].

Que signifie "avoir connaissance du caractère illicite d'un contenu" ? Cela est assez réglementé donc ne vous faîtes pas trop de souci : vous devez seulement laisser aux utilisateurs un moyen de vous signaler tout contenu illicite selon des conditions bien précises[26]. Un formulaire d'exemple est disponible en annexe. En revanche, vous avez l'obligation de signaler à la police tout contenu signalé par un utilisateur de cette manière et de bloquer l'accès à ce contenu une fois qu'il est avéré que le contenu est effectivement illicite.

La direction générale de la police nationale (office central de lutte contre la criminalité liée aux TIC) ou un juge peut également vous adresser une demande de retrait de contenu à laquelle vous devez obligatoirement vous soumettre.

Rappelons qu'en dehors du signalement par un utilisateur, d'une requête judiciaire ou d'une demande de la police, vous n'avez pas obligation de surveiller les contenus hébergés[27] **et que chercher à le faire peut constituer une atteinte à la vie privée.**

[23] https://owncloud.org/
[24] Article 6 I 2° de la LCEN
[25] Article 6 II de la LCEN
[26] Article 6 I 5° de la LCEN
[27] Article 6 7° de la LCEN

b) Bases de données : CNIL et obligations

Lorsque vous proposez à vos adhérents un service d'annuaire ou un service reposant sur une base de données, ou lorsque votre association utilise une base de données pour gérer ses abonnés, ou même lorsque vous stockez les *logs* de connexion pendant un an, vous relevez du régime de la base de données régulé par la CNIL (Commission Nationale Informatique et Libertés).

Toute base de données doit obligatoirement être déclarée auprès de la CNIL chaque année, mais il existe quelques dispenses détaillées sur leur site Internet[28]. Toutes les procédures se font en ligne. En particulier, il est obligatoire de déclarer une base de donnée comportant des données dites sensibles (origines raciales ou ethniques, opinions politiques, philosophiques ou religieuses, état de santé, vie sexuelle, infractions, condamnations ou mesures de justice, informations sur les difficultés sociales, numéro de sécurité sociale).

Un certain nombre d'obligations vous incombent concernant les bases de données et les données personnelles :

- les personnes dont vous recueillez des données personnelles doivent en être informées au moyen d'un encart disponible en annexe, et peuvent exercer leurs droits sur ces données
- vous devez assurer la sécurité et la confidentialité des données
- les données recueillies doivent avoir une date de péremption et ne peuvent être conservées indéfiniment
- les données recueillies doivent l'être avec une finalité précise et indiquée aux personnes. Utiliser les données pour une autre finalité est une infraction.
- les bases de données ainsi constituées doivent être, sauf dispense, déclarées à la CNIL chaque année

c) Noms de domaines

Avec les noms de domaine, il existe souvent un risque de contrefaçon (vous ne pouvez pas utiliser un nom de domaine si la marque associée existe déjà) et de concurrence déloyale (une marque ne peut se créer si un nom de domaine existe antérieurement). Il est donc conseillé, dans le cas précis ou le nom de domaine permet une activité commerciale ou de communication de grande envergure, et qu'il existe un risque de contrefaçon, de déposer la marque associée à l'INPI[29] en même temps que la création du nom de domaine. Cela n'est bien sûr pas utile pour les sites Internet des associations de votre campus ou les sites Internet temporaires.

d) Mentions légales

Il est obligatoire de faire figurer pour chaque site Internet un lien vers des mentions légales : elles sont détaillées par la CNIL et doivent comprendre le nom et la forme sociale de la personne qui est responsable du site Internet, le nom de la personne responsable de son édition (responsable de son contenu), et le nom et la forme sociale de la personne responsable de son hébergement. On trouvera en annexe un exemple de mentions légales. N'hésitez pas à en parler aux membres ou associations qui hébergent des sites Internet chez vous !

[28] https://www.cnil.fr/
[29] https://www.inpi.fr/fr

IV Compléments juridiques et fiscaux

a) Si vous êtes un club BdE

Si votre association n'est pas une association loi 1901 mais ce qu'on appelle un club ou une section d'une autre association comme un BdE ou une Association des Élèves, alors vous n'avez pas de personnalité morale. C'est à dire que vous dépendez du président du BdE qui est le responsable légal de votre activité. Si vous êtes FAI, alors il faut déclarer le BdE tout entier à l'ARCEP !

b) Si vous avez des clubs subordonnés

Parfois vous avez les ressources nécessaires pour financer d'autres activités associatives : club d'électronique, club de développement, fab lab, club de robotique, club de radiodiffusion etc. Attention à la structure juridique que vous adoptez : il est beaucoup moins contraignant d'un point de vue fiscal que ces activités soient de simples clubs sans personnalité morale ! Il est alors très facile d'effectuer des transferts d'argent sur différents comptes qui dépendent tous du trésorier de votre association. Si vous financez d'autres associations loi 1901, il est tout de suite plus délicat de leur transférer de l'argent car il faut une validation par votre Conseil d'Administration et une déclaration au fisc de ces transferts qui sont imposés !

c) Assurance de matériel et locaux

Pensez à faire assurer vos locaux et votre matériel si aucune assurance n'est incluse avec l'achat. Pensez également à faire assurer les événements que vous organisez auprès d'assureurs pour professionnels. Posez-vous la question, en cas de partage de locaux, de la responsabilité des uns et des autres : si quelqu'un d'extérieur à l'association provoque un incendie dans un de vos locaux techniques, qui est responsable, et qui paye la facture ? Vous pouvez discuter de ces détails avec le gestionnaire de la résidence.

d) Impôts commerciaux et TVA

En tant qu'association loi 1901, vous n'êtes pas soumis aux impôts commerciaux dont la TVA et l'IS (http://www.associations.gouv.fr/701-l-association-et-les-impots.html), sous certaines conditions. Renseignez-vous auprès de votre centre des impôts le plus proche ou en préfecture pour vous faire exonérer ! Cela bien entendu si vous êtes déjà déclarés au fisc et que vous payez des impôts tous les ans. Si vous êtes exonérés d'impôts, vous avez même le droit à 60000€ d'activités lucratives complémentaires (bénéfices de ventes, places à un événement etc).

Il peut être avantageux fiscalement de revoir votre modèle de cotisation afin de rentrer dans le plafond de 60000€ : conserver une petite partie de cotisation et considérer le reste comme une participation aux frais techniques. Sur un montant initial de 50€, vous pourriez avoir une cotisation à l'association de 10€, et 40€ de frais facturés à l'adhérent pour qu'il ait Internet ou qu'il accède aux services que vous proposez. Vous trouverez un exemple de facture en annexe. Ce modèle vous permet de toucher 10€ de cotisation par adhérent qui ne sont pas taxés par l'État et 40€ par adhérent qui ne sont pas taxés car leur total n'excède pas la limite de 60000€.

V Annexes

En annexe sont rassemblés des *templates* de documents utilisables par les associations pour la plupart de leurs démarches. N'hésitez pas à vous en inspirer !

Il est toujours préférable de faire vérifier l'ensemble de vos documents auprès d'un conseil juridique : demandez aux juristes de votre école ou à vos professeurs de droit en cas de souci particulier !

Exemple de demande écrite de déclaration à l'ARCEP

Voir en ligne sur arcep.fr, espace opérateur, pour effectuer la déclaration. Il vous faudra joindre une demande écrite signée dont voici un exemple :

Eugene Dupont
Président d'ASSORESO
2, allée des Onduleurs
59200 Tourcoing

Tourcoing, le 28 mars 2016

Objet : demande écrite de déclaration de nos activités à l'ARCEP

Madame, Monsieur,

En tant que président d'ASSORESO, j'ai l'honneur de vous adresser un formulaire de déclaration de nos activités auprès de l'ARCEP.

Je vous prie d'agréer Madame, Monsieur l'expression de mes salutations les plus distinguées.

Eugene Dupont

Date et signature

Exemples d'articles à insérer dans les statuts des associations FAI

Une fois déclarés à l'ARCEP, si vous êtes une association loi 1901, il est conseillé d'ajouter quelques précisions dans vos statuts.

- Déjà dans vos objets sociaux, vous pouvez ajouter celui-ci :

Définir, réglementer, mettre en œuvre les utilisations du réseau en assurant leur cohérence et leur respect des cadres législatifs et réglementaires

- Et ajouter un article comme suit :

Article X – Statut de Fournisseur d'accès Internet L'association est régulièrement déclarée auprès de l'Autorité de Régulation des Communications Électroniques et des Postes (ARCEP), et fait donc partie des Fournisseurs d'Accès Internet français répertoriés par l'ARCEP. Elle répond ainsi à l'ensemble des exigences légales définies par les articles L32 et suivants du Code des Postes et des Communications Électroniques.

Compléments juridiques sur les obligations de faire et de ne pas faire des FAI

NOTES JURIDIQUES

-

OBLIGATIONS DE FAIRE ET DE NE PAS FAIRE INCOMBANT AUX OPERATEURS ET FOURNISSEURS D'ACCES A INTERNET

-

Le présent document s'attache à présenter de manière claire et synthétique les obligations qui incombent aux opérateurs, en s'appuyant sur les cadres législatif et réglementaire au niveau national et européen. L'accent est particulièrement porté sur les opérateurs qui relèvent du régime de fournisseur d'accès Internet et non d'opérateur de téléphonie fixe ou mobile, en soulignant les dispositions relatives aux données à caractère personnel et au respect de l'intimité de la vie privée des utilisateurs. On donne en dernière page un EPILOGUE afin de résumer les différentes obligations de faire et de ne pas faire détaillées dans les sections suivantes.

SECTION 1 - DEFINITIONS

Opérateur : un opérateur est une personne physique ou morale exploitant un réseau de communications électroniques ouvert au public ou fournissant au public un service de communications électroniques[30].

Accès à Internet : l'accès à Internet est l'ensemble des moyens mis à disposition d'un bénéficiaire pour connecter un équipement terminal au réseau informatique public mondial et émettre et recevoir des transmissions électroniques à destination de ce réseau.

Fournisseur d'accès Internet (FAI) : un FAI est un opérateur proposant à un ensemble de bénéficiaires un accès à Internet en tant que service de communications électroniques.

SECTION 2 - OBLIGATIONS AUPRES DE L'AUTORITE DE REGULATION DES COMMUNICATIONS ELECTRONIQUES ET DES POSTES

L'Autorité de régulation des communications électroniques et des postes (ARCEP) est une autorité administrative indépendante dont les compétences sont définies[31] dans le Code des postes et des communications électroniques (CPCE). Les activités de communications électroniques incluant l'activité de fourniture d'accès Internet s'exercent librement à la condition d'avoir effectué une déclaration préalable de ces activités auprès de l'ARCEP[32].

L'ARCEP est habilitée[33] à contrôler ou faire contrôler par un tiers, aux frais des opérateurs, le respect des obligations fixées en application de la loi[34]. Ces obligations portent, sans s'y limiter, sur les conditions de qualité, sécurité, confidentialité, neutralité et accès aux données personnelles.

[30] Article L32 15° du Code des postes et des communications électroniques (CPCE)
[31] Articles L32 et L32-1 du CPCE
[32] Articles L32-1 I 1° et L33-1 du CPCE
[33] Article L33-12 du CPCE
[34] Articles L33-1, L36-6, L42-1 du CPCE

L'ARCEP est habilitée à demander la communication de toute convention liée à l'exploitation d'un réseau en termes d'interconnexion et d'accès signée par l'opérateur[35]. Ces informations pourront être communiquées sur demande aux tiers intéressés, sous réserve des informations couvertes par le secret des affaires.

SECTION 3 – UTILISATION DE FREQUENCES RADIOELECTRIQUES

L'utilisation par un opérateur de fréquences radioélectriques est régulée et définie selon les dispositions du CPCE[36]. Les bandes de fréquences sont attribuées par décret aux administrations de l'État ou à l'administration de l'ARCEP[37]. Le spectre des fréquences relève du domaine public de l'État[38] et son utilisation est une occupation du domaine public soumise à une autorisation administrative. Il est fait mention de fréquences libres[39] dont l'utilisation n'est pas soumise à une autorisation administrative et dont la liste est publiée par l'ARCEP. Elle inclut à ce jour les bandes de fréquence 2.4Ghz et 5Ghz dans des conditions précisées par l'ARCEP[40]. Leur utilisation reste soumise à la déclaration préalable auprès de l'ARCEP.

Un opérateur a l'interdiction d'exploiter des bandes de fréquences radioélectriques pour lesquelles il n'est pas muni d'une autorisation administrative.

SECTION 4 - CONSERVATION ET EXPLOITATION DES DONNEES A CARACTERE PERSONNEL

Est une donnée à caractère personnel toute donnée relative à une personne physique identifiée ou identifiable[41].
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[42], mais peuvent différer d'une durée maximale d'un an les opérations visant à anonymiser ou effacer ces données techniques, à des fins de poursuite d'infractions pénales et qui sont fournies à la seule demande des autorités habilitées, dont le détail est fourni au paragraphe suivant[43]. Ces données doivent permettre l'identification de l'émetteur et des destinataires de la communication électronique et les données liées aux équipements terminaux mis en œuvre à ces fins[44], avec une durée de conservation d'un an à compter du jour de leur enregistrement.
Ces données techniques ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications[45].

[35] Article D99-6 du CPCE
[36] Articles L41 et suivants du CPCE
[37] Article L41 du CPCE
[38] Article L41-1 du CPCE
[39] Articles L33-3 et L42 du CPCE
[40] http://arcep.fr/uploads/tx_gspublication/guide-juridique-crip2007.pdf
[41] Article 2 bis de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
[42] Article L34-1 II du CPCE
[43] Article L34-1 III du CPCE
[44] Article R10-13 du CPCE
[45] Article L34-1 VI du CPCE

Les données conservées en vue de la sécurité des réseaux et des installations ne peuvent, elles, être conservées que pour une durée maximale de trois mois[46].

Une demande de communication de données relatives au trafic peut être adressée au fournisseur d'accès Internet par une autorité habilitée : il s'agit des services de gendarmerie nationale et de police nationale dans le cadre de la prévention du terrorisme[47], de la Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet[48] et de l'autorité nationale de sécurité des systèmes d'information[49]. Le Procureur de la République peut enfin, dans le cadre d'une procédure pénale ou d'une enquête, autoriser un agent ou un officier de la police judiciaire à demander au fournisseur d'accès Internet la communication de toute donnée informatique en sa possession[50].

Fournir à un tiers non autorisé des données à caractère personnel, incluant sans s'y limiter les données relatives au trafic permettant l'identification, est une infraction[51]. Le fait pour un fournisseur d'accès Internet de consulter et d'exploiter les données relatives au trafic dans un objectif différent de sa mission première de fourniture d'accès Internet est une infraction[52].

SECTION 5 - PROTECTION DE LA VIE PRIVEE DES UTILISATEURS DE SERVICES ELECTRONIQUES

Est une violation de données à caractère personnel toute violation de la sécurité entraînant 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[53].
En cas de violation de données à caractère personnel, le fournisseur d'accès Internet notifie, sans délai, la Commission nationale de l'informatique et des libertés.
Lorsque cette violation peut porter atteinte aux données à caractère personnel ou à la vie privée d'un abonné ou d'une autre personne physique, le fournisseur avertit également, sans délai, l'intéressé.

Dans le cadre d'une procédure pénale, un juge d'instruction peut autoriser des agents de la police judiciaire à mettre en place un dispositif technique afin de capter toutes les données transmises et reçues par un utilisateur d'un système de traitement automatisé de données[54], tandis que le Procureur de la République peut autoriser un agent ou un officier de la police judiciaire à demander au fournisseur d'accès Internet la communication de toute information issue d'un système informatique[55].

Hors de la procédure pénale, l'interception de correspondances électroniques émises ou reçues depuis un équipement terminal sans consentement de l'auteur est encadrée par le Code de la

[46] Article R10-14 du CPCE
[47] Article L34-1-1 du CPCE
[48] Article L331-12 du Code de la propriété intellectuelle
[49] Article L2321-1 du Code de la défense
[50] Article 77-1-1 du Code de procédure pénale
[51] Article 226-22 du Code pénal
[52] Article 226-21 du Code pénal et article L34-1 III du CPCE
[53] Article 34 bis de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
[54] Article 706-102-1 du Code de procédure pénale
[55] Article 77-1-1 du Code de procédure pénale

sécurité intérieure et ne peut être exécutée qu'à la demande des services spécialisés de renseignement décrétés par le Premier ministre et avec son autorisation[56]. Elle est ensuite menée par des agents individuellement désignés et habilités et par les opérateurs[57]. Les services spécialisés de renseignement ainsi décrétés sont la direction générale de la sécurité extérieure, la direction de la protection et de la sécurité de la défense, la direction du renseignement militaire, la direction générale de la sécurité intérieure, le service à compétence nationale dénommé "direction nationale du renseignement et des enquêtes douanières" et le service à compétence nationale dénommé "traitement du renseignement et action contre les circuits financiers clandestins"[58]. Les finalités de ces interceptions concernent entre autres la défense nationale, la prévention du terrorisme et la prévention de la criminalité organisée et de la délinquance organisée[59].

Chacun a droit au respect de sa vie privée[60].
En dehors de ces procédures exceptionnelles et sérieuses, qu'elles soient pénales ou administratives, la mise en place d'un dispositif technique permettant d'ouvrir, détourner ou prendre frauduleusement connaissance de correspondances électroniques[61], ou permettant une atteinte à la vie privée d'autrui en captant ou enregistrant des paroles prononcées à titre privé[62] est une infraction. Ainsi toute tentative d'inspection de communications électroniques à destination d'un réseau de communication par le fournisseur d'accès Internet ne disposant pas d'une requête de l'autorité judiciaire ou administrative habilitée est une infraction.

Il est enfin à noter que la responsabilité des fournisseurs d'accès Internet ne saurait être engagée, civilement et pénalement, à raison des contenus transmis sur les réseaux de communications[63].

SECTION 6 - FILTRAGE DES COMMUNICATIONS ELECTRONIQUES

Le filtrage préventif des communications électroniques reposant sur une inspection de leur contenu est une infraction telle que précisée dans la section précédente. Le fournisseur d'accès Internet a cependant la responsabilité de procéder au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique dès qu'il en reçoit la demande par l'autorité administrative compétente[64]. Cette autorité compétente est la direction générale de la police nationale, Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication[65].

Il est à noter que les fournisseurs d'accès Internet proposant de manière complémentaire un service d'hébergement de contenus à leurs abonnés sont tenus, à la demande de l'autorité

[56] Article L852-1 du Code de la sécurité intérieure
[57] Tables du Conseil d'État 2015 sur le Droit au respect de la vie privée, section 4.3
[58] Décret n° 2015-1185 du 28 septembre 2015 portant désignation des services spécialisés de renseignement
[59] Article L811-3 du Code de la sécurité intérieure
[60] Article 9 du Code civil
[61] Article 226-15 du Code pénal
[62] Article 226-1 du Code pénal
[63] Article L32-3-3 du CPCE
[64] Article 6-1 de la Loi pour la confiance dans l'économie numérique (LCEN)
[65] Décret n° 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique

suscitée ou bien dès qu'ils en ont connaissance, et sous certaines conditions, de procéder au retrait des contenus litigieux[66].

La Cour de Justice de l'Union Européenne confirme que la liberté d'entreprendre, la liberté d'expression, et le respect de la vie privée protégé par le droit communautaire s'opposent à une injonction faite à un fournisseur d'accès à Internet de mettre en place à titre préventif un système de filtrage de toutes les communications électroniques transitant par ses services, notamment par l'emploi de logiciels «peer-to-peer»[67].

Le projet de loi pour une république numérique prévoit enfin une obligation du respect de la neutralité de l'Internet pour les fournisseurs d'accès Internet[68] qui inclut une obligation de traitement égal et non discriminatoire des communications électroniques, conformément aux directives européennes en vigueur[69].

EPILOGUE

Le fournisseur d'accès Internet se déclare à l'ARCEP et obéit à ses injonctions dans le cadre des pouvoirs qui lui sont conférés.

Le fournisseur d'accès Internet n'exploite que les bandes de fréquences radioélectriques pour lesquelles il est muni d'une autorisation administrative, ou exploite les fréquences ne requérant pas d'autorisation.

Le fournisseur d'accès Internet a pour obligation de conserver de manière confidentielle les données d'identification relatives au trafic de ses abonnés pendant une durée d'un an. Il transmet ces informations à la seule demande des autorités compétentes, et s'expose à des poursuites pénales en cas de divulgation à un tiers non autorisé.

Le fournisseur d'accès Internet ne procède à aucun filtrage ni analyse du contenu des communications électroniques à titre préventif et s'expose à des poursuites pénales dans le cas contraire. Le fournisseur d'accès Internet met cependant ponctuellement en place tout dispositif d'interception requis par les autorités compétentes, dans le cadre de la sécurité intérieure uniquement et sur autorisation du Premier ministre.

Le fournisseur d'accès Internet bloque l'accès aux sites indiqués par l'autorité compétente et bloque l'accès à tout contenu litigieux dès qu'il en a connaissance sous certaines conditions.

[66] Article 6 de la LCEN
[67] Arrêt de la CJUE, 24 novembre 2011, SABAM C/ Scarlet Extended
[68] Article 11 du projet de loi pour une République Numérique
[69] Proposition de règlement du Parlement européen et du Conseil établissant des mesures relatives au marché unique européen des communications électroniques et visant à faire de l'Europe un continent connecté, et modifiant les directives 2002/20/CE, 2002/21/CE et 2002/22/CE ainsi que les règlements (CE) n° 1211/2009 et (UE) n° 531/2012

Exemple de facture pour les adhérents

Voici un exemple de facture que vous pouvez fournir à vos adhérents au moment de leur adhésion et que vous devez conserver :

FACTURE - ASSORESO

ASSORESO
2, allée des Onduleurs
59200 Tourcoing
SIRET : 123 456 789 00012

0123456789
tresorier@assoreso.fr

A : Pierre Jacques

Date : Le 28/03/2016 à 12h34

Facture n° : 123

Désignation	**Qté**	**Prix unitaire €**	**Prix total €**
Cotisation pour 1 an	1	10,00	10,00
Frais d'accès Internet pour 12 mois	1	40,00	40,00

Total **Votre règlement**	50,00€ 50,00€
A PAYER	0,00€

(TVA non applicable, article 293 B du CGI)

Exemple de charte de bonne utilisation du réseau à faire signer aux adhérents

Voici un exemple de document à annexer à votre Règlement Intérieur, à faire signer à vos adhérents au moment de leur adhésion au format papier ou de manière électronique. N'hésitez pas à le modifier selon vos propres besoins !

ASSORESO – CHARTE DE BON COMPORTEMENT DU RESEAU MIS A DISPOSITION

1. L'adhérent est responsable de ses fichiers et de l'intégrité de son espace de travail.
2. L'adhérent est le seul responsable de ses activités et des contenus qu'il consulte ou produit à destination du réseau.
3. L'adhérent s'engage à respecter la législation en vigueur et notamment concernant la propriété intellectuelle. Il s'engage à ne pas partager de logiciel ou de contenu multimédia sans le consentement de son auteur.
4. La connexion consentie à l'adhérent est strictement personnelle. Il s'engage sous peine de radiation à ne pas partager ou céder cette connexion à un tiers.
5. L'adhérent est le seul responsable de l'utilisation qui est faite de ses appareils électroniques. Il pourra être tenu responsable de toute utilisation qui en faite, avec ou sans son accord.
6. L'adhérent s'engage à notifier à l'association ASSORESO toute tentative de piratage ou de vol de ses appareils électroniques et de ses comptes.
7. L'adhérent s'engage à respecter la vie privée des autres utilisateurs du réseau.
8. L'adhérent s'engage à ne pas troubler le bon fonctionnement du réseau mis à sa disposition.
9. L'adhérent comprend que l'association ASSORESO peut, à la demande de l'autorité judiciaire, produire toutes les données en sa possession permettant de l'identifier.
10. L'adhérent s'engage à respecter le Règlement Intérieur de l'association ASSORESO et comprend que sa radiation et des poursuites pourront être engagées si nécessaires.

Je soussigné(e)……, utilisateur des moyens informatiques et réseaux de ASSORESO, déclare avoir pris connaissance des conditions ci-dessus et m'engage à les respecter.

Fait à le

Signature

Exemple de réponse aux ayants droits

C'était un piège ! **Rappel : on ne répond pas aux avertissements et messages des ayant droits**.

Exemple de charte à faire signer aux utilisateurs d'un hébergement Web ou de fichiers

Lorsque vous proposez un service d'hébergement de fichier ou d'hébergement Web, il est conseillé de joindre au Règlement Intérieur une charte de bonne utilisation de ces services ou de faire signer un document de cette nature à l'utilisateur.

ASSORESO – CHARTE DE BONNE UTILISATION DU SERVICE D'HEBERGEMENT MIS A DISPOSITION

1. L'utilisateur est le seul responsable des fichiers et contenus qu'il enregistre sur son espace de stockage ou d'hébergement Web.
2. L'utilisateur s'engage à respecter la législation en vigueur et notamment concernant la propriété intellectuelle. Il s'engage à ne pas partager de logiciel ou de contenu multimédia sans le consentement de son auteur.
3. L'utilisateur s'engage à signaler tout contenu illicite à ASSORESO dès qu'il en a connaissance, selon le formulaire précisé dans le Règlement Intérieur.
4. L'utilisateur s'engage à notifier à l'association ASSORESO toute tentative de piratage ou de vol de son espace d'hébergement. Il s'engage à notifier toute compromission de données personnelles qui pourraient s'y trouver.
5. L'utilisateur s'engage à respecter la vie privée des autres utilisateurs du réseau.
6. L'utilisateur s'engage à ne pas publier ou télécharger de contenu illicite vers ou depuis son espace d'hébergement ou les espaces d'hébergement des autres utilisateurs.
7. L'utilisateur s'engage à ne pas troubler le bon fonctionnement du service d'hébergement mis à sa disposition.
8. L'utilisateur comprend que l'association ASSORESO peut, à la demande de l'autorité judiciaire, produire toutes les données en sa possession permettant de l'identifier.
9. L'utilisateur s'engage, lorsqu'il héberge un site Internet, à y faire apparaître des mentions légales conformément à la règlementation en vigueur.
10. L'utilisateur s'engage à respecter le Règlement Intérieur de l'association ASSORESO et comprend que sa radiation et des poursuites pourront être engagées si nécessaires.

Je soussigné(e)……, utilisateur du service d'hébergement de fichiers ou de site Internet mis à disposition par ASSORESO, déclare avoir pris connaissance des conditions ci-dessus et m'engage à les respecter.

Fait à le

Signature

Encart obligatoire sur les données personnelles

A chaque fois que vous récoltez des données personnelles de la part de vos adhérents, il est obligatoire de faire apparaître les mentions suivantes. Plus de détails sur le site de la CNIL.

Responsable du traitement : Paul Dupont.

Les informations portées sur ce formulaire sont facultatives (*obligatoires*). Elles font l'objet d'un traitement informatisé destiné à ..... [*préciser la finalité*]. Les destinataires des données sont : …… [*préciser*].

Conformément à la loi "informatique et libertés" du 6 janvier 1978 modifiée, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent. Si vous souhaitez exercer ce droit et obtenir communication des informations vous concernant, veuillez-vous adresser à …… [*préciser le service chargé du droit d'accès*]

Vous pouvez également, pour des motifs légitimes, vous opposer au traitement des données vous concernant [*à ne pas faire figurer si le traitement présente un caractère obligatoire*].

Templates de mentions légales

Tout site Internet doit faire figurer des mentions légales. Attention, se renseigner pour les cas spécifiques[70]. Les exemples suivants sont les exemples minimum, mais il faut dans certains cas indiquer davantage d'informations.

- Pour un site d'un professionnel (entreprise, association) à des fins commerciales ou non :

Société (ou entrepreneur individuel)	**Hébergeur**	**Responsable du contenu**
Nom	Nom	Prénom NOM
Dénomination, raison sociale, forme juridique	Dénomination ou raison sociale	
Adresse du siège	Adresse du siège	
Numéro de téléphone	Numéro de téléphone	
Adresse de courrier électronique		
SIREN/SIRET		

- Pour un site d'un particulier (site personnel, blog etc) à des fins non commerciales :

Créateur du site	**Hébergeur**
Prénom NOM	Nom
Adresse du domicile	Dénomination ou raison sociale
Numéro de téléphone	Adresse du siège
	Numéro de téléphone

[70] https://www.service-public.fr/professionnels-entreprises/vosdroits/F31228

Formulaire de déclaration de contenu litigieux

Lorsque vous proposez à vos utilisateurs un service d'hébergement de fichiers ou Web, il est obligatoire de fournir aux utilisateurs un moyen de signaler tout contenu illicite ou litigieux. Voici le formulaire tel que défini dans la Loi pour la confiance dans l'économie numérique[71].

FORMULAIRE DE NOTIFICATION DE CONTENU ILLICITE POUR DEMANDE DE RETRAIT

Date de notification :

Notification émise à destination de l'association ASSORESO, association loi 1901 établie au 2, allée des Onduleurs, 59200 Tourcoing, France.

Remplir si vous êtes une personne physique :	*Remplir si vous êtes une personne morale :*
Nom :	Forme :
Prénoms :	Dénomination :
Profession :	Siège social :
Domicile :	Organe qui vous représente légalement :
Nationalité :	
Date et lieu de naissance :	

Description des faits litigieux et localisation précise :

Motifs pour lesquels le contenu doit être retiré, comprenant la mention des dispositions légales et des justifications de faits :

Merci de joindre à ce formulaire une copie de la correspondance adressée à l'auteur ou à l'éditeur des informations ou activités litigieuses demandant leur interruption, leur retrait ou leur modification, ou la justification de ce que l'auteur ou l'éditeur n'a pu être contacté.

J'ai conscience que je m'expose à des poursuites au titre de l'article 6, I, 4° de la Loi pour la confiance dans l'économie numérique en cas de demande de retrait abusive alors que je sais que les informations que je porte dans ce formulaire sont inexactes.

Fait à , le Signature

[71] Article 6 de la LCEN