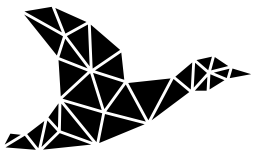

netCommons.eu

Internet en libre accès

obligations en matière de vie privée et de liberté de communication

À jour en date du 29 janvier 2018

Ce guide juridique s'adresse aux organisations qui, en France, fournissent un accès à Internet de façon ouverte (par Wi-Fi, hot-spot, par câble ou sur postes fixes) : locaux associatifs, bibliothèques, centres d'information, résidences collectives, universités, bars, hôtels, magasins, cybercafés, etc.

Ce guide tente de répondre à trois questions qui se posent à elles en matière de vie privée et de liberté de communication :

– Quels sites peuvent-elles bloquer ?
– Quelles informations peuvent-elles collecter sur les personnes utilisant le service ?
– Quelles informations doivent-elles obligatoirement conserver ?

Ce guide ne s'adresse ni aux organisations qui fournissent un accès sur abonnement, ni aux individus qui partagent leur accès à Internet (dans le cadre d'une sous-location, par exemple), ni aux organisations qui fournissent un accès à un réseau fermé (un intranet).

A. Quels sites peuvent être bloqués ?

Neutralité du Net

Les organisations concernées par ce guide sont tenus de respecter la **neutralité du Net**[1], qui leur interdit de réaliser toute « restriction » quant aux « contenus consultés ou diffusés » par les utilisateurs. Par exception, la neutralité du Net permet le blocage de deux types de contenus :

– ceux qui mettent en danger la **sécurité** du service ou du terminal des personnes qui l'utilisent ;
– ceux dont le blocage est **exigé par la loi**.

Une organisation qui ne respecterait pas la neutralité du Net (en bloquant un site n'entrant pas dans une des exceptions) encourrait une **amende** égale à 3% de son chiffre d'affaire ou, s'il n'a pas d'activité commerciale, à **150 000 €**[2].

Blocage exigé par la loi

S'agissant du blocage exigé par la loi, il ne peut résulter que d'une décision judiciaire ou administrative visant des contenus précis : aucune loi n'impose aux organisations de bloquer des contenus sans décision individualisée.

De plus, certaines lois qui limitent habituellement la circulation de l'information ne s'imposent pas à ces organisations.

En premier lieu, la loi **HADOPI** exige de surveiller son accès à Internet pour éviter qu'il ne serve à commettre des actes de contrefaçon[3]. Or, cette loi **ne s'impose qu'aux utilisateurs et utilisatrices** finales qui bénéficient de l'accès et non aux personnes qui le fournissent. En effet, en droit, « les personnes dont l'activité est d'offrir un accès [à Internet] ne sont pas soumises à [...] une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites »[4].

En deuxième lieu, constitue un délit le fait de mettre à disposition de **personnes mineures** des contenus « à caractère violent, incitant au terrorisme, pornographique ou de nature à porter gravement atteinte à la dignité humaine »[5]. Néanmoins, la loi prévoit aussi que la responsabilité (civile ou pénale) des personnes qui fournissent un « accès à un réseau de communications électroniques » ne peut être engagée à raison des contenus qu'elles diffusent[6]. Elles ne sont donc pas concernés par ce délit et, ainsi, **ne sont pas tenues de bloquer** les contenus concernés.

À la place, ces organisations doivent informer leurs utilisateurs et utilisatrices « de l'existence de moyens techniques permettant de restreindre l'accès » à certains sites (des logiciels de filtrage) et leur proposer un de ces moyens à utiliser[7], notamment pour protéger les mineurs. De plus, lorsqu'une organisation met des **postes fixes** à disposition du public, son activité dépasse la simple fourniture d'accès à Internet et nous lui conseillons donc d'y installer un filtre et/ou d'exiger la présence d'un adulte afin de protéger les mineurs.

Exception

La neutralité du Net ne s'impose qu'aux personnes qui offrent un accès à Internet « au public » (qui, en droit, sont alors qualifiées d'opérateurs[8]). Ceci exclut les personnes qui n'offrent cet accès qu'à un **« groupe d'utilisateurs prédéfini »**[9]. Cette notion est encore floue, et nous proposons de l'interpréter comme un groupe n'étant pas susceptible d'évoluer constamment et librement. Ainsi, par exemple, nous considérons que ne serait **pas soumise à la neutralité du Net** une entreprise qui ne fournirait un accès qu'à ses salariés (et pas aux autres personnes), dès lors que le groupe des salariés ne peut être librement rejoint par toute personne.

À l'inverse, nous considérons, par exemple, que **doit respecter la neutralité du Net** une bibliothèque qui, bien que ne fournissant un accès qu'aux personnes inscrites ou disposant d'une carte, permettrait à toute personne de s'inscrire ou d'obtenir une telle carte. Dans ce dernier cas, le fait que la carte soit payante ou soumise à une condition d'âge ne nous semble pas constituer un critère suffisamment discriminant pour qu'on puisse parler d'un « groupe d'utilisateurs prédéfini » et échapper à la neutralité du Net.

Confidentialité des communications

Peu importe que la loi impose ou non aux organisations de respecter la neutralité du Net, celles-ci doivent systématiquement respecter la **confidentialité des communications** de leurs utilisateurs. La loi interdit toute mesure « d'interception ou de surveillance » des communications électroniques ainsi que des données de trafic nécessaires à la diffusion de ces communications[10]. Cette interdiction connaît les mêmes exceptions que la neutralité du Net (la sécurité ou l'obligation de la loi) ainsi qu'une troisième : le consentement des utilisatrices et utilisateurs (néanmoins, il est peu probable que les ceux-ci acceptent d'être surveillés, d'autant que l'accès à Internet ne peut leur être dénié s'ils s'y refusent[11]).

Nous considérons que le blocage de sites Internet implique certaines opérations (analyse et traitement de l'adresse des sites auxquels tentent d'accéder chaque personne) qui pourraient correspondre à des atteintes à la confidentialité des communications. À ce titre aussi, en dehors des exceptions prévues par la loi, nous conseillons à toute organisation de ne bloquer aucun site. Ne pas respecter la confidentialité des communications est passible d'une amende de **225 000 €** et d'un **an d'emprisonnement**[12].

---

[1] Le principe de la neutralité du Net est défini à l'article 3 du règlement 2015/2120 de l'Union européenne.

[2] Les atteintes à la neutralité du Net sont sanctionnées à l'article L. 36-11 du code des postes et des communications électroniques (CPCE).

[3] Le régime de responsabilisation prévue par la loi HADOPI est prévu à l'article L. 336-3 du code de propriété intellectuelle.

[4] L'absence d'obligation des fournisseurs d'accès à Internet de surveiller les contenus est garantie à l'article 6, I, point 7, de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

[5] Le délit de mise à disposition de mineurs de certains contenus est défini à l'article l'article 227-24 du code pénal.

[6] Le régime de responsabilité limité des fournisseurs d'accès à Internet est prévu à l'article L. 32-3-3 du CPCE. Il prévoit qu'un fournisseur n'est responsable des contenus qu'il diffuse que si il est « à l'origine de la demande de transmission litigieuse », « sélectionne le destinataire de la transmission » ou « sélectionne ou modifie les contenus faisant l'objet de la transmission ».

[7] L'obligation de proposer des filtres aux utilisateurs est prévue à l'article 6, I, point 1, de la loi du 21 juin 2004

[8] En application de l'article L. 32 du code des postes et des communications électroniques, est opérateur « toute personne physique ou morale exploitant un réseau de communications électroniques ouvert au public ou fournissant au public un service de communications électroniques ».

[9] La notion de groupe d'utilisateurs prédéfini est détaillée au points 10 à 12 des lignes directrices du BEREC quant à l'application de la neutralité du Net, traduites par l'ARCEP

[10] La confidentialité des communications électroniques est garantie à l'article 5 de la directive 2002/58 de l'Union européenne, en partie transposé aux articles L. 32-3 et L. 34-1 du CPCE.

[11] La CNIL considère que « le refus de consentir ne doit pas empêcher la personne d'accéder au service » .

[12] La peine sanctionnant les atteintes à la confidentialité des communications est prévue à l'article 226-15 du code pénal, devant être portée au quintuple s'agissant des personnes morales

B. Quelles informations peuvent être collectées ?

La collecte de **données personnelles**[13] La collecte de données personnelles[13] (telles que le nom ou l'adresse d'une personne) n'est autorisée qu'à cinq conditions[14] :

– avec le **consentement** de la personne (mais les personnes refusant de consentir ne doivent pas être empêchées d'accéder à Internet[11]) ;
– pour exécuter un éventuel **contrat** conclu avec la personne ;
– pour exécuter une **mission de service public** à laquelle participe l'organisation ;
– pour exécuter une **obligation légale** ;
– en raison d'un **« intérêt légitime »**.

Cet « intérêt légitime » n'autorise que les opérations qui sont effectivement utiles pour l'organisation ou pour des tiers, et dont l'utilité est plus importante que l'atteinte portée à la vie privée des personnes concernées. S'agissant de l'exécution d'une mission de service public ou d'un contrat, la collecte de données personnelles doit être indispendable à cette exécution.

Par exemple, recueillir l'identité d'une personne porte atteinte à sa vie privée mais n'est souvent d'aucune utilité pour les organisations qui fournissent un accès libre à Internet. En effet, **aucune loi n'impose aux fournisseurs d'accès à Internet de recueillir l'identité** des personnes utilisant leur service[15] et ne saurait donc justifier une telle collecte (ce n'est que dans des cas exceptionnels qu'un fournisseur d'accès à Internet peut être obligé de collecter l'identité des utilisateurs et utilisatrices, lorsqu'un juge le lui ordonne précisément[16]).

De même, dans la mesure où les fournisseurs d'accès à Internet ne sont **pas responsables** des faits commis par les personnes utilisant l'accès[6], ils n'ont aucun intérêt personnel à pouvoir identifier les personnes qui commettent des actes illégaux via cet accès, ni donc aucun intérêt à collecter l'identité de tous les utilisateurs et utilisatrices pour y parvenir.

Au contraire, dans les cas où, pour une raison particulière, une organisation souhaiterait ne fournir l'accès qu'à un groupe limité de personnes (celles payant un prix, par exemple), et si cette limitation ne peut pas être réalisée autrement (en donnant le mot de passe unique qui permet d'accéder au réseau, par exemple), l'organisation pourrait avoir un intérêt à obtenir l'identité des personnes qui accèdent au service (mais elle devra alors se limiter à collecter les seules informations indispensables à cette fin).

Pour mettre en place une telle restriction, l'organisation doit toutefois pouvoir démontrer que l'objectif poursuivi (sécurité, facturation, etc.) ne peut pas être poursuivi au moyen d'une autre méthode n'impliquant pas de collecte d'identité.

Les organisations qui collectent ou traitent des données personnelles sans y être autorisées encourent une amende de **20 000 000 €** ou 4 % du chiffre d'affaire mondial[17].

Enfin, comme expliqué plus tôt, les communications et données de trafic ne peuvent être traitées que pour des raisons de sécurité, sur l'ordre de la loi ou avec l'autorisation de l'utilisateur ou utilisatrice.

---

[13] Une « donnée personnelle » est toute information qui porte sur un individu et qui peut être associée à cet individu, de façon directe ou indirecte.

[14] Les conditions de licéité d'un traitement de données personnelles sont listées à l'article 7 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[15] La CNIL a pu rappeler que « le cybercafé en question n'est pas obligé de relever et de conserver l'identité de ses clients pour fournir une connexion (ex : accès Wi-Fi ouvert) » (voir l'article « Conservation des données de trafic : hot-spots wi-fi, cybercafés, employeurs, quelles obligations ? » du 28 septembre 2010 sur cnil.fr).

[16] Par exemple, en application de l'article L. 336-2 du code de propriété intellectuelle, un juge peut ordonner à un fournisseur d'accès à Internet de faire cesser une infraction commise grâce à l'accès qu'il fournit. Le fournisseur peut alors choisir de mettre fin à cette atteinte en sécurisant, par exemple, son réseau à l'aide d'un mot de passe confié à certaines utilisatrices et utilisateurs, une telle mesure ayant été reconnue dans son principe comme conforme au droit européen par la Cour de justice de l'Union européenne (CJUE, McFadden, 15 septembre 2016, affaire C-484/14).

[17] À partir du 25 mai 2018, les traitements illicites pourront être sanctionnés par une amende maximale de 20 000 000 € ou 4% du chiffre d'affaire mondial, en application de l'article 83 du règlement général sur la protection des données.

C. Quelles informations doivent être conservées ?

Droit français

La loi française prévoit que toute organisation fournissant un accès à Internet doit conserver pendant un an[18] les informations suivantes :

– l'**identifiant du terminal** des personnes utilisant le service (telle que l'adresse MAC de son terminal, utilisée pour lui fournir l'accès) ;
– un **identifiant attribué** à chaque personne et à sa connexion (telle que l'adresse IP attribuée à chaque terminal) ;
– les **dates et heures** de début et de fin de l'accès à Internet fourni à chaque personne ;
– les **caractéristiques de la ligne** attribuée à chaque personne[19].

La loi française sanctionne le non-respect de ces obligations d'une peine d'un **an d'emprisonnement** et d'une amende de **375 000 €**[20].

Par ailleurs, les données conservées ne doivent en aucun cas concerner le **contenu** des informations reçues ou envoyées par les utilisateurs ou utilisatrices, et doivent se limiter au **strict minimum** de ce qui est requis[21], sans quoi il s'agirait d'une atteinte à la confidentialité des communications décrites ci-avant.

Enfin, dans les seuls cas où elle y est autorisée (dans les conditions exposées ci-avant), une organisation qui décide de recueillir de façon habituelle certaines informations doit conserver celles-ci pendant un an[22]:

– le nom et le pseudonyme de l'utilisateur ou utilisatrice;
– son adresse postale ou électronique;
– son numéro de téléphone ;
– le hash du mot de passe associé à la connexion;
– lorsque l'accès est payant, le type de paiement utilisé, la référence du paiement, le montant et la date et l'heure de transaction.

Cette obligation de conservation est soumise à la même peine que l'obligation générale.

Droit européen

La **Cour de justice** de l'Union européenne (UE) considère[23] que la Charte des droits fondamentaux de l'Union européenne **interdit aux États de l'UE** d'adopter une loi qui :

– impose « une **conservation généralisée** et indifférenciée de l'ensemble des données [...] de tous les abonnés et utilisateurs » ;
– « oblige les fournisseurs [...] à conserver ces données de manière **systématique et continue** » ;
– « s'applique donc même à des personnes pour lesquelles il n'existe **aucun indice** de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions pénales graves » ;
– « ne requiert **aucune relation** entre les données dont la conservation est prévue et une menace pour la sécurité publique ».

Nous considérons donc que l'obligation de conservation imposée aux fournisseurs d'accès à Internet français est contraire à la Charte de l'UE. Cette Charte étant **hiérarchiquement supérieure** aux lois françaises, les hébergeurs français ne devraient être obligés de conserver aucune donnée : or, conserver des données personnelles sans justification est puni en droit européen d'une amende de **20 000 000 €** ou 4% du chiffre d'affaire mondial[17].

En conséquence, tant pour respecter le droit que les personnes qui utilisent leurs services, **nous recommandons aux organisations d'appliquer le droit européen**.

Cependant, une organisation peut avoir un besoin légitime de conserver certaines données pour des raisons techniques et de sécurité. Ainsi, pour la durée strictement nécessaire, elle peut conserver les données techniques (adresses MAC et IP, dates et heures de connexion) impérativement nécessaires pour des raisons techniques et de sécurité.

---

[18] L'obligation imposée aux fournisseurs d'accès à Internet de conserver des données est prévue par l'article L. 34-1 du CPCE (détaillé par le décret n° 2011-219 du 25 février 2011). Ces deux textes ont des conséquences très proches pour les organisations visées par le présent guide, et sont donc ici présentées conjointement. Le premier de ces deux textes concerne tout type de communications électroniques, et non le seul accès à Internet : il vise ainsi des données qui concernent d'autres types de communications (des communications téléphoniques), notamment des données liées à des « services complémentaires » et à des « destinataires » qui ne concerne pas l'accès à Internet et ne doivent pas à être prises en compte par les organisations visées par ce guide.

[19] Dans le cadre du présent guide, l'obligation de conserver « les caractéristiques de la ligne attribuée à l'utilisateur » ne devrait concerner que les organisations qui fournissent un accès à Internet par cable et qui ont attribué un identifiant unique à chacune des prises qu'elles mettent à disposition du public, ce qui n'est généralement fait que pour répondre à des impératifs de sécurité particuliers.

[20] L'article L39-3 du CPCE et l'article 131-38 du code pénal fixent la sanction attachée à la conservation des données, qui doit être portée au quintuple s'agissant des personnes morales.

[21] La CNIL rappelle l'obligation de ne conserver que les données strictement requises, regrettant que de nombreuses personnes en conservent plus que nécessaire (voir l'article « Internet et wi-fi en libre accès : bilan des contrôles de la CNIL » du 22 décembre 2014 sur cnil.fr).

[22] L'obligation de conserver les données spontanément collectées est prévue à l'article 6, paragraphes II et VI, de la loi du 21 juin 2004

[23] Arrêt Tele2 Sverige (C-203/15) de la Cour de justice de l'Union européenne du 21 décembre 2016, dont sont ici cités les paragraphes 97, 105, 106 et 108.