La responsabilité pénale des fournisseurs de services Internet

Avis de la Police fédérale, avril 2000

1. Remarque préalable

Le 23 juillet 1998, la Police fédérale a envoyé une circulaire aux fournisseurs de services Internet (*Internet Service Providers, ISP*) de Suisse leur demandant de tester le blocage de certains sites ayant un contenu de discrimination raciale au sens de l'art. 261bis du code pénal suisse[1] (CP). Cette demande était motivée par le fait que faciliter l'accès à de tels sites pouvait être qualifié de complicité (art. 25 CP) à une infraction principale. Cette circulaire a déclenché un tollé général de la part des ISP, ce qui a entraîné la création d'un groupe de contact qui devait tenter de concilier les intérêts des fournisseurs d'accès à Internet, d'une part, et ceux des autorités policières de la Confédération, d'autre part. **Ce groupe de contact se compose actuellement d'une représentation des ISP suisses et de représentants des offices fédéraux de l'informatique, de la communication, de la justice et de la police.**

Les efforts visant à empêcher la diffusion et la consultation de contenus illicites sur Internet doivent aussi tenir compte du fait que les **besoins de communication légitimes** doivent pouvoir être satisfaits sans entrave[2] sur Internet. Il faut également susciter **l'intérêt de l'économie** pour la place suisse et, par conséquent, pour des conditions générales comparables au niveau international[3] en ne négligeant pas la **mission légale des autorités policières et judiciaires** consistant à poursuivre ou à empêcher les délits perpétrés sur Internet[4]. Il ne faut pas oublier que beaucoup de délits doivent être poursuivis d'office et que, pour une grande partie des délits, la compétence de poursuite et de jugement **relève des cantons**.

Le présent avis doit également servir à **répondre aux questions fondamentales relatives à la responsabilité pénale des ISP et à indiquer les voies possibles pour la collaboration avec les autorités de poursuite pénale**. Ce document doit être considéré comme un complément au rapport établi par un groupe de travail interdépartemental en mai 1996.[5]

Après qu'une première ébauche du présent document a été mise en consultation auprès des membres du groupe de contact, il a fallu obtenir **l'avis d'un expert sur la question de la responsabilité pénale des fournisseurs d'accès Internet,**

[1] RS 311.0

[2] Cf. les libertés d'opinion et d'information prévues par l'art. 16 de la Constitution fédérale (Cst.) du 18.4.1999, entrée en vigueur le 1.1.2000.

[3] Voir p. ex. le plan d'action élaboré par le Secrétariat d'Etat à l'économie (SECO) pour la promotion du commerce électronique en Suisse.

[4] La liberté économique garantie par la Constitution (art. 27 et 94 Cst.) ne peut être restreinte que dans les cas et conditions prévus par l'art. 36 Cst.; en l'occurrence et en premier lieu par les dispositions légales du CP.

[5] Internet, Le Nouveau Média Interroge Le Droit; rapport d'un groupe de travail interdépartemental sur des questions relevant du droit pénal, du droit de la protection des données et du droit d'auteur suscitées par Internet. (http://www.ofj.admin.ch/themen/ri-ir/internet/rf-internet-f.pdf).

conformément aux art. 27 et 322bis CP. Dans l'intervalle, l'avis a été rédigé par l'Office fédéral de la justice (OFJ) et distribué dans le groupe de travail[6]. Il y sera fait allusion par la suite aux endroits appropriés.

2. Délits sur Internet

Internet reflète au moins en partie le monde réel avec ses aspects fascinants et ses aspects moins sympathiques. C'est ainsi qu'Internet et ses nombreux services sont désormais utilisés pour presque tous les types d'actes criminels. Les actes punissables peuvent être répartis en deux groupes principaux:

- **Les délits perpétrés par le transfert de données (souvent à court terme) via Internet**. Tombent dans cette catégorie les délits informatiques à proprement parler, tels que la soustraction de données (art. 143 CP), l'accès indu à un système informatique (art. 143bis CP), la détérioration de données (art. 144bis CP), l'utilisation frauduleuse d'un ordinateur (art. 147 CP) ainsi que l'obtention frauduleuse d'une prestation (art. 150, al. 3, CP). Viennent encore s'ajouter tous les autres délits au cours desquels des informations sont transmises via Internet, tels que la violation des droits d'auteur, l'infraction à la loi sur les loteries, la violation du secret de fabrication ou du secret commercial (art. 162 CP), l'espionnage (art. 272 ss. CP), le blanchiment d'argent (art. 305bis CP), etc. Cette catégorie peut également accueillir les autres délits de participation (complicité, assistance, instigation) à tous les délits possibles lorsqu'ils existent dans la communication entre les complices.
- **Les délits perpétrés par l'intermédiaire d'Internet durant un certain temps, en donnant à consulter des contenus punissables.** Entrent dans cette catégorie, par exemple, la représentation de la violence (art. 135 CP), l'escroquerie (art. 146 CP; p. ex. par la tromperie au moyen d'un site Web), la pornographie (art. 197 CP), les délits qui sont poursuivis sur plainte, comme les délits contre l'honneur (art. 173 ss. CP), la discrimination raciale (art. 261bis CP) et les violations des droits d'auteur[7].

Pour les infractions de la première catégorie, la phase de l'acte passant via Internet n'est constatable que par une surveillance simultanée du transfert des données. En d'autres termes, il n'est pas envisageable d'empêcher ou de limiter l'entrée de données par des mesures spécifiques à Internet, de sorte que seuls des types d'intervention traditionnels peuvent laisser escompter des résultats.

La deuxième catégorie revêt un intérêt particulier car les actes punissables qui y sont répertoriés se produisent souvent pendant une certaine durée, si bien que leur découverte et la prise de mesures adéquates permettent au moins de limiter la portée du délit. **En ce qui concerne les délits relatifs à Internet souvent débattus dans l'opinion publique, soit la pornographie et la discrimination raciale, on constate que les contenus punissables se trouvent généralement sur des serveurs étrangers**[8].

[6] L'avis peut être consulté sur Internet: http://www.bj.admin.ch/themen/ri-ir/access/intro-d.htm.
[7] Cf. annexe 2 du rapport du groupe de travail interdépartemental de mai 1996.
[8] Cette remarque vaut surtout pour le WWW tandis que les contenus des groupes d'information se retrouvent aussi fréquemment sur des serveurs d'information (*New-Server*) en Suisse.

La lutte contre la criminalité multiple sur Internet ne peut se contenter de la création de cyberpoliciers mais nécessite (en plus) la constitution d'un savoir spécialisé pour les autorités de poursuite pénale compétentes.

3. Les acteurs d'Internet[9]

Les différentes personnes et organisations actives sur Internet peuvent être classées dans les groupes suivants (toutefois, les limites sont parfois floues et certaines personnes peuvent remplir plusieurs fonctions) :

- **Utilisateurs / Users**: les personnes qui demandent les services proposés sur Internet.
- **Opérateurs / Carriers**: ils exploitent l'infrastructure de base pour relier les segments de réseau (systèmes de transmission et lignes). Il s'agit par exemple de Swisscom, Sunrise ou diAx[10].
- **Network-Providers**: les personnes ou organisations qui louent l'infrastructure de transmission de base (lignes louées) aux opérateurs et qui, à l'aide de routeurs, exploitent des réseaux complexes qui permettent aux ISP de se connecter à Internet (ex.: ip-plus, Eunet, etc.)[11].
- **Fournisseurs de services Internet (ISP)**: ils permettent à l'utilisateur d'accéder à Internet (au sens de la fonction de **fournisseur d'accès** / ***Access-Provider***) et proposent aussi généralement des services, par exemple via des serveurs Web, de messagerie ou d'informations (p. ex.: Swiss Online, Bluewin, Datacomm, etc.). En l'occurrence, l'intérêt porte particulièrement sur la fourniture d'accès (**fournisseurs d'accès**) et la mise à disposition de capacité de stockage sur les serveurs Web (**fournisseurs d'hébergement / *Hosting-Providers***).
- **Fournisseurs de services en ligne** ou **Online-Service-Providers**: à la différence des ISP, ils offrent principalement des services "propriétaires" (en particulier offres de données) qu'ils enregistrent sur des ordinateurs personnels et qui ne peuvent être consultés que par les abonnés du service en ligne. Ils assument en plus la fonction d'ISP. Les fournisseurs de services en ligne seront confondus par la suite avec l'appellation "fournisseurs d'accès Internet" ou ISP. Les exemples les plus connus sont AOL et Compuserve.
- **Fournisseurs de contenu** ou **Content-Providers**: les personnes qui rendent accessibles des informations personnelles sur les serveurs d'ISP ou des services en ligne (ou sur leur propre ordinateur). Il peut s'agir, par exemple, de l'auteur d'un article pour un groupe de discussion (newsgroup) ou une entreprise présente sur le Web.

---

[9] Cf. les commentaires d'Ulrich Sieber dans l'article "Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen", dans Computer und Recht 10/97, p. 597, ainsi que les explications d'Andreas Ochsenbein et de Peter L. Heinzmann dans l'étude "Strafrechtliche Aspekte im Internet", dans Kriminalistik 7/98, p. 516 s.

[10] Tant pour les opérateurs que pour les fournisseurs de réseau, il faut retenir que, principalement pour des raisons d'organisation par couche de l'architecture de réseau, il n'existe pas de mesures de contrôle ou d'ingérence fondées pénalement (voir Ulrich Sieber, "Verantwortlichkeit im Internet", Beck'sche Verlagsbuchhandlung, Munich 1999, p. 27).

[11] Cf. note 9

4. Applications Internet (services)

Selon qu'une application Internet est publique ou que l'auteur d'une information ne veut atteindre que les destinataires désignés par lui, les applications les plus fréquentes peuvent être réparties comme suit :

- **Publiques** : WWW, groupes d'informations accessibles librement, serveurs FTP (autant que l'accès n'est pas limité), forums de discussion accessibles librement.
- **Non publiques** et donc protégées par le secret des télécommunications[12] dont: E-mails[13], groupes de discussion privés, téléphonie via Internet[14].

5. Types de responsabilité pénale

L'avis de droit de l'OFJ mentionné dans l'introduction indique de manière précise sur la base de quelles dispositions du CP la responsabilité pénale d'un fournisseur d'accès peut être engagée. Les considérations de cet avis peuvent aussi servir à déduire la responsabilité pénale pour les autres fonctions d'un ISP et des autres fonctions sur Internet.

Pour résumer, l'avis stipule les **points suivants :**

- **Tous les délits relatifs au contenu des médias n'entraînent pas une application du droit pénal des médias.** En sont exclus notamment les délits visés par les art. 135 (représentation de la violence), 197 (pornographie) et 261bis du CP (discrimination raciale)[15] (pt 4.3 de l'avis).
- En ce qui concerne les délits relatifs au contenu des médias menant à l'application du droit pénal des médias, **seul l'auteur[16] est en principe punissable**. Cela vaut également pour Internet (pts 5.2.1 et 5.3.1).
- En vertu du système du droit pénal des médias (art. 27 en relation avec l'art. 322bis CP), il est obligatoire **d'indiquer une personne responsable de la publication, même en l'absence de l'auteur**. Il peut et doit être tenu compte de l'éventuelle relative responsabilité de la personne plus éloignée dans l'ordre des responsabilités lors de l'application de l'art. 322bis CP (pt 5.2.2 *in fine*).
- Le **fournisseur d'hébergement** peut être considéré comme le **responsable secondaire** éventuel pour ce qui est des personnes actives sur Internet et du droit pénal des médias (pt 5.3.3.2).
- ”S'il "est absent" comme personne secondairement responsable, il semble légitime de considérer le **fournisseur d'accès** comme **responsable secondaire** (pts 5.3.3.3. et 5.3.4). Dans ce cas, il faut fixer certaines limites, au besoin très étroites (pt 5.3.3.4).

---

[12] Art. 13, al. 1, Cst.; art. 43 de la loi sur les télécommunications (LTC/RS 784.10)
[13] Sur plainte de droit public de la société Swiss Online SA, le Tribunal fédéral est parvenu à la conclusion le 5.4.2000 (numéro de dossier 1A.104/1999) que le trafic des e-mails était protégé par le secret des télécommunications et qu'il ne peut être surveillé que dans les conditions prévues à l'art. 179^{octies} CP (cf. NZZ du 6.4.2000).
[14] Les groupes d'utilisateurs privés généralement créés sur un Intranet ou Extranet peuvent aussi être considérés comme non publics. Selon la taille et la structure, il est possible néanmoins de considérer dans ce groupe un caractère public, au sens de l'art.261bis CP par exemple.
[15] L'arrêt du Tribunal fédéral cité dans le rapport sous le numéro de dossier 6S. 810-813/1998 a depuis été publié sous la référence 125 IV 206.
[16] Au sens des fonctions répertoriées sous le point 3, il s'agit des fournisseurs de contenu.

- En ce qui concerne la connaissance relative à un contenu spécifique sur Internet nécessaire pour qualifier les **actes** visés par l'art. 322bis CP **d'intentionnels**, il n'est ni possible ni raisonnable pour le fournisseur d'accès d'effectuer lui-même les contrôles. **Les informations de tiers** sur de tels contenus **doivent être concrètes et émaner d'une source fiable** (pt 6.1.2).
- La connaissance, pertinente sur le plan juridique, du fournisseur d'accès relativement à un contenu délictueux ne peut être reconnue que si l'information correspondante émane d'une **instance de procédure pénale**, par exemple d'un juge d'instruction ou d'un procureur. Les simples affirmations de particuliers ou les communiqués de presse généraux ne peuvent généralement pas suffire pour prouver une connaissance pertinente quant à l'intention (pt 6.1.2).
- La réalisation intentionnelle de l'état de fait visé par l'art. 322bis CP par un fournisseur d'accès est certes possible mais cela ne se produit pas fréquemment dans la pratique. **Il est plus probable** que l'on soit confronté à des cas où il faut traiter avec **une intention éventuelle** (pt 6.1.4).
- En ce qui concerne l'**acte de négligence** de l'art. 322bis CP, le devoir d'agir en toute diligence se fonde notamment sur le degré de risque général où toute personne qui crée une situation de risque doit tout mettre en œuvre pour que ce danger n'entraîne pas la violation de biens juridiques de tiers. **Le fournisseur d'accès doit mettre en œuvre tout ce qui est raisonnablement possible pour que l'utilisateur final n'ait pas accès aux contenus délictueux** (pt 6.2.2).
- **L'acceptabilité se mesure par des critères objectifs et les rapports personnels** (pt 6.2.3). Ces derniers doivent être déterminés au cas par cas pour chaque malfaiteur (point 6.2.3.2).
- Pour ce qui est des circonstances objectives, le devoir de diligence du fournisseur (d'accès) ne s'applique généralement que si ce dernier détient une **information concrète et fiable sur un contenu délictueux**, ce qui est le cas lorsque le renseignement émane d'une autorité suisse de poursuite pénale (pt 6.2.3.1).
- En raison du caractère qualifié de la connaissance préalable, **une réalisation par négligence de l'état de fait visé par l'art. 322bis CP ne se produit que dans de rares cas exceptionnels** (pt 6.2.4).
- **Pour résumer, on peut retenir à propos de l'étendue de la responsabilité du fournisseur d'accès que sa position de responsable à titre subsidiaire ou de "second rang" a une influence très limitée sur la portée réelle de sa responsabilité pénale: il ne peut être admis ou supposé à la légère qu'il connaisse le contenu délictueux, mais des informations concrètes doivent être fournies par les autorités suisses de poursuite pénale** (pt 6.3).
- La punissabilité du fournisseur d'accès en matière de délits créés par le contenu des médias qui ne tombent pas sous le coup des dispositions spéciales du droit pénal des médias suit les **règles générales de participation** selon lesquelles les fournisseurs d'accès peuvent être punis de complicité pour une infraction principale s'ils ne prennent pas les mesures requises malgré la connaissance du contenu délictueux sur Internet (pt 7).
- La connaissance du contenu délictueux par le fournisseur est déterminante pour la reconnaissance d'une complicité répréhensible car celle-ci ne peut être réalisée qu'intentionnellement (pt 7).

- Il ne peut être demandé au fournisseur d'accès, comme complice possible, de surveiller les contenus transitant par son installation. **La connaissance de l'existence de certains contenus punissables** doit lui être apportée par la remarque de tiers (pt 7).
- L'information donnée par une autorité de poursuite pénale au fournisseur d'accès relativement à des contenus concrets du réseau doit être jugée comme suffisante. Les communications faites par des personnes privées ne devraient remplir qu'exceptionnellement les conditions requises (pt 7).

En ce qui concerne la participation possible évoquée du fournisseur d'accès comme complice de l'auteur d'une infraction principale, il faut par ailleurs se référer au point 1.5 de l'avis de droit selon lequel la doctrine déterminante postule une application - souvent illimitée - du principe d'ubiquité (art. 7 CP) aux délits suscités par Internet, lesquels sont fréquemment conçus comme des délits matériels (*Erfolgsdelikte*). En l'occurrence, **le droit pénal suisse est applicable, quand bien même - comme c'est souvent le cas - l'infraction principale a été commise à l'étranger**[17].

Pour ce qui est de l'argument voulant qu'une complicité possible n'entre pas en ligne de compte parce que le service fourni par le fournisseur d'accès représente un acte neutre de tous les jours, il faut se référer au point 5.3.3.4 de l'avis précisant que le Tribunal fédéral a rejeté ce type de considération appliquée aux réseaux de communication.

Face à ces considérations de l'OFJ s'appliquant en premier lieu aux fournisseurs d'accès, les compléments suivants doivent être apportés pour ce qui a trait aux **fournisseurs d'hébergement**:

Le fournisseur d'hébergement est lié par un contrat avec le fournisseur de contenu pour ce qui est de la capacité de stockage mise à disposition sur le serveur Web. En ce qui concerne le droit pénal des médias, il est donc aussi considéré comme responsable secondaire[18] (pts 5.3.3.2 de l'avis de droit de l'OFJ).

Comme pour le fournisseur d'accès, **la connaissance revêt aussi une importance prépondérante pour le fournisseur d'hébergement** pour concrétiser l'intention d'un acte au sens de l'art. 322bis CP. Cette connaissance est également nécessaire pour faire appliquer le devoir de diligence dans le cas de la commission par négligence (voir avis du BJ, pt 6.2.4).

Outre les informations provenant de sources concrètes et fiables fondant la responsabilité pénale d'un fournisseur d'hébergement, une autre question se pose pour savoir si des informations moins qualifiées suffisent ou s'il faut présumer qu'il appartient au fournisseur d'hébergement de contrôler lui-même le contenu de son serveur Web. Ces questions s'appliquent principalement aussi aux fournisseurs qui mettent à disposition gratuitement des capacités de stockage de leur serveur Web ou qui permettent au fournisseur de contenu un accès non vérifié.

Etant donné que le **contenu du serveur Web** d'un fournisseur d'hébergement est déterminé et modifié en général par le fournisseur de contenu sans l'aide du fournisseur d'hébergement, la connaissance des contenus par ce dernier ne pourrait s'acquérir que par des contrôles régulièrement répétés. Vu les énormes quantités de

[17] En ce qui concerne l'infraction au sens de l'art. 322bis CP, la question de l'infraction principale préalable ne se pose pas car l'art. 322bis CP concerne une infraction autonome (avis de l'OFJ ; pt 5.3.3.4).
[18] Le principe de la responsabilité primaire et exclusive du fournisseur de contenu / auteur s'applique naturellement ici aussi.

données contenues sur un serveur Web, de tels contrôles relèveraient de la gageure et ne peuvent donc pas être imposés[19]. Il se peut néanmoins que le fournisseur d'hébergement, à de rares occasions, doive émettre des doutes fondés quant à la légalité de l'utilisation faite de la capacité de stockage mise à la disposition du fournisseur de contenu, et ce sur la base d'informations obtenues, par exemple, lors de la conclusion du contrat avec le fournisseur de contenu. Dans ce cas, il peut lui être imposé de **contrôler** les contenus de ce fournisseur **au moins par sondage**, pour ne pas se voir accusé de complicité intentionnelle (éventuelle).

Comme le volume de données stockées sur le serveur Web est moins grand que celui transitant par l'infrastructure d'accès et que le fournisseur d'hébergement est le suivant dans la chaîne des intermédiaires entre le fournisseur de contenu et l'utilisateur, il doit être exigé du fournisseur d'hébergement qu'il recherche - contrairement au fournisseur d'accès - des informations détaillées et concrètes même si elles ne proviennent pas d'une source pouvant être assimilée à une instance de procédure pénale. Ce **devoir supplémentaire - rechercher des informations - du fournisseur d'hébergement par rapport au fournisseur d'accès** se justifie moins par des raisons de proximité technique avec le fournisseur de contenu que par le fait que les deux parties se trouvent liés contractuellement. Dans certains cas, ces informations peuvent conduire à ce que le fournisseur d'hébergement doivent faire des recherches supplémentaires avec l'aide d'une autorité répressive ou de tiers professionnellement qualifiés[20,21]. Mais régulièrement, l'estimation parallèle dans la sphère non professionnelle devrait suffire pour répondre à la question de savoir si un contenu déterminé est punissable. Pour cela, le fournisseur d'hébergement doit évaluer, en tenant compte de ses vues, de son environnement et de l'interprétation des dispositions légales, si un contenu doit être considéré comme non autorisé[22].

Il reste à ajouter au sujet de ces explications qu'elles ne concernent - d'un point de vue pénal - le fournisseur d'hébergement que si le fournisseur de contenu ne peut pas être trouvé ou qu'il ne peut pas être poursuivi en justice dans notre pays.

Pour ce qui est de la participation à des délits ne tombant pas sous le coup des dispositions spéciales du droit pénal des médias, on peut ajouter aux développements de l'avis de droit de l'OFJ les éléments suivants pour le fournisseur d'hébergement:

On ne parle généralement **que de la complicité** au sens de l'art. 25 CP[23] comme forme de participation possible. La proximité fonctionnelle et juridique du fournisseur d'hébergement et du fournisseur de contenu ainsi que la quantité de données plus réduite sur son serveur Web – par rapport au volume de données transitant par le fournisseur d'accès – a pour conséquence, au niveau de l'élément de connaissance de la complicité intentionnelle, qu'il faut exiger de lui la même attitude que celle prévue à l'art. 322bis CP: il faut rechercher, en plus des informations qualifiées provenant des autorités de poursuite pénale, des renseignements détaillés et concrets émanant d'autres sources.

---

[19] Voir aussi Ochsenbein / Heinzmann, loc. cit., p. 602 ss.
[20] Cf. Internet, Le Nouveau Média Interroge le Droit, loc. cit., p. 10 ss. (les commentaires qui y sont faits se rapportent, il est vrai, à la complicité et non au droit pénal des médias; ils peuvent néanmoins être utilisés pour l'élément de connaissance d'un acte au sens de l'art. 322bis CP)
[21] Le risque de "censure privée" dont il est question dans l'avis de l'OFJ (pt 6.1.2) et qui peut être craint en raison de la diminution de la demande de qualité des informations n'est pas aussi présent dans les rapports entre les fournisseurs de contenu et d'hébergement car, en vertu de la liberté de contrat, le fournisseur d'hébergement est libre de mettre son serveur à la disposition de qui il veut et pour quoi.
[22] Schultz, AT I CP, 4e édition, Berne 1982, p. 190 s.
[23] Voir Internet, Le Nouveau Média Interroge Le Droit, loc. cit., p. 8

Dans les développements exposés jusqu'ici, il a surtout été question des contenus du World Wide Web. **Mais, d'un point de vue pénal, la même chose vaut en principe aussi pour les contenus des serveurs d'informations ou FTP**.

S'agissant des contenus diffusés sur des serveurs d'informations, une surveillance active n'est pas envisageable à cause des énormes volumes de données et des contenus sans cesse variables[24]. Pour autant qu'un serveur d'informations ne contienne pas exclusivement des groupes de la branche, la liberté d'information interdit le blocage de l'accès à un tel serveur. Il faut cependant exiger de l'exploitant de serveurs d'informations qu'il recherche des renseignements détaillés et concrets sur les groupes dont les sites ont un contenu punissable. Comme les contenus d'un groupe présentent souvent de grandes différences qualitatives, un renseignement sur des messages isolés d'un groupe ne permet pas de fonder l'exactitude de la connaissance, d'autant que les différents messages sont automatiquement effacés au bout d'une période relativement courte. Mais si on peut déduire de cette information que des messages au contenu punissable sont régulièrement et principalement envoyés dans un groupe, il faut vérifier l'information et au besoin supprimer ce groupe (ainsi qu'empêcher sa réapparition automatique).

En ce qui concerne les **serveurs FTP**, les questions de responsabilité pénale se posent en premier lieu à l'exploitant d'un tel serveur, alors que la possibilité d'un blocage ciblé de l'accès (à certains répertoires ou fichiers) peut être exclu par le fournisseur d'accès en raison des particularités techniques[25]. L'exploitant d'un serveur FTP qui autorise le stockage libre de données doit faire son enquête. On ne peut cependant attendre de lui à ce niveau qu'il utilise, pour lire les fichiers, des logiciels qui ne peuvent être considérés comme habituels pour sa branche.

Il est clair que la question d'un blocage d'accès ou d'un contrôle de contenu n'entre pas en ligne de compte pour les **serveurs de discussion Internet** (Internet Relay Chat-Server). La rapidité du passage des données ne permet pas d'établir une connaissance pénalement pertinente[26].

6. Aspects techniques d'un blocage d'accès[27]

Des questions techniques complexes se posent au sujet de l'accès à des contenus illicites de serveurs WWW en raison de leur large diffusion et de la présence relativement longue des contenus sur les serveurs. Comme déjà mentionné, il faut partir du principe que l'auteur réel ou le fournisseur d'hébergement ne peut légalement pas être poursuivi dans de nombreux cas (ex.: les serveurs localisés aux USA et au Canada sont protégés par la liberté d'expression). C'est pourquoi la "deuxième meilleure" solution consiste en un blocage de l'accès à de tels contenus par les fournisseurs suisses d'accès à Internet ou de réseau.

De quelles possibilités un fournisseur de services Internet dispose-t-il pour bloquer un contenu déterminé sur un serveur WWW?

---

[24] Cf. Ulrich Sieber, Verantwortlichkeit im Internet, p. 51

[25] Le blocage de l'accès à tout un serveur FTP est à peine imaginable car celui-ci contient généralement aussi des fichiers non punissables pénalement.

[26] Voir à ce sujet Ulrich Sieber, Verantwortlichkeit im Internet, p. 40 ss. et 57 ss.

[27] Pour les aspects techniques, voir Rosenthal, David: Current Problems and Possible Strategies for Combating Racism on the Internet (http://www.rvo.ch/docs/unracism.pdf), ainsi que Sieber Ulrich: Verantwortlichkeit im Internet – Technische Kontrollmöglichkeiten und multimediarechtliche Regelungen (Beck: Munich 1999).

1. Le fournisseur **bloque l'adresse IP** du serveur Web concerné au niveau du routeur. Cette mesure entraîne le blocage de *toutes* les offres présentes sur le serveur et non pas seulement le contenu incriminé. Cette procédure n'est donc pas une solution praticable pour les gros fournisseurs tels que AOL ou Geocities qui contiennent des milliers de contenus différents. Elle convient davantage aux offres illicites ayant leur propre serveur / nom pour lesquelles un nom de domaine déterminé ou une adresse IP précise ne présente que des contenus similaires (p. ex. racistes ou extrémistes violents). Dans le cas des contenus racistes et extrémistes, cette situation est relativement fréquente car ces fournisseurs de contenu veulent tirer avantage de noms de domaine faciles à retenir (p. ex.: stormfront.org, aryanbooks.com). Les sites Web que la Police fédérale recommande actuellement de bloquer correspondent à cette catégorie.
   Une variante de cette solution consiste à exclure certains noms de domaine (tels que stormfront.org) au niveau du DNS (Domain Name Server ou serveur de nom de domaine).
2. Le fournisseur exploite un **serveur proxy**. Toutes les consultations du WWW (p. ex.: Port 80) entrent dans la configuration de base du navigateur Web via ce proxy. Ce dernier permet alors l'enregistrement des consultations, le stockage temporaire des données demandées mais aussi leur blocage. Le client doit configurer son navigateur Web en conséquence. S'il ne le fait pas, le serveur proxy est contourné et la communication est établie directement avec le site souhaité. La plupart des fournisseurs exploitent de tels serveurs proxy, mais dans le but d'accroître les performances. Il existe également des proxies pour d'autres protocoles que le http, comme par exemple le FTP.
3. Le fournisseur utilise un "**proxy transparent**", de sorte que les clients se servent automatiquement du serveur proxy, qu'ils le veuillent ou non. Dans le proxy, il est possible d'instaurer un blocage jusqu'au niveau d'une page précise. En principe, il s'agit ici d'un firewall ouvert qui peut dévier et éventuellement filtrer certains services[28].

Une modification de la variante 1 est aujourd'hui utilisée pour interdire l'accès à des sites Web dont le blocage est recommandé par la Police fédérale.

Toutes les variantes ont néanmoins en commun **certains inconvénients**:

a) Tous les types de filtrage entraînent des **problèmes de performance**, les méthodes pouvant difficilement évoluer. Ce qui fonctionne correctement pour une douzaine d'adresses mène à une interruption de l'infrastructure du fournisseur pour quelques millier d'autres.

b) Toutes les méthodes citées peuvent être contournées par l'utilisation d'un **anonymizer** qui masque l'adresse IP du contenu recherché.

c) L'expérience montre que les sites Web bloqués sont stockés par la communauté Internet sur plusieurs serveurs en copie intégrale (**mirroring** ou mise en miroir) car de tels procédés sont interprétés – presque par réflexe - par beaucoup d'utilisateurs comme une censure. Tous ces sites Web ont dû à nouveau être bloqués.

d) Le **coût** de mise à jour et de gestion de listes de blocage est élevé pour les fournisseurs. La méthode de blocage entraîne également des investissements élevés

[28] Un problème identique se pose néanmoins ici comme pour les serveurs proxy normaux. Selon les paramètres, il bloque l'accès à des services utilisant des protocoles ou des ports spéciaux (p. ex.: le télébanking).

variant selon le procédé choisi. Plus de 300 fournisseurs actifs sont actuellement recensés en Suisse, les grandes entreprises et les administrations publiques / écoles n'étant pas prises en compte. Même pour les services policiers / juridiques demandant les blocages, les frais administratifs ne doivent pas être sous-estimés. Une aide pourrait être apportée jusqu'à un certain degré par le blocage au niveau des fournisseurs de réseau sur lesquels s'appuie tout ISP.

e) Une solution nationale est en principe problématique dans le monde d'Internet. Grâce aux tarifs téléphoniques relativement bas actuellement, un client suisse peut choisir un fournisseur étranger (sans blocages). Certains fournisseurs de services en ligne (p. ex.: AOL) proposent en plus, d'après leurs propres indications, l'accès à Internet dans toute l'Europe via le même réseau; dans ce cas, un blocage uniquement valable pour la Suisse ne serait pas réalisable avec cette topologie de réseau.

Bilan de l'aspect technique:

Le blocage de sites Web complets (nom de domaine ou adresse IP) est réalisable pour les fournisseurs de services Internet ou pour les réseaux mais ne convient pas dans tous les cas (si le contenu illicite ne représente qu'une partie de l'offre, p. ex. pour les sociétés d'hébergement sur le Web) et est très onéreux selon la méthode choisie.

Les inconvénients de toutes les solutions techniques au niveau national sont les efforts administratifs et financiers relativement élevés ainsi que la possibilité de contournement par l'utilisateur qui ne recule pas devant une dépense certaine. L'effort administratif nécessaire de la part des fournisseurs pourrait cependant être réduit si **une seule instance** était désignée en Suisse pour les blocages et si cette instance mettait régulièrement à disposition les données nécessaires (adresses IP, noms de domaine) dans un **format lisible par les machines**. Si les grands **fournisseurs suisses de réseau** (comme ip-plus, Eunet, etc.) effectuaient les blocages à titre de service pour leurs clients, la grande majorité des plus petits fournisseurs qui tirent leur capacité de ligne des fournisseurs de réseau en bénéficieraient automatiquement. Cette solution n'éliminerait toutefois pas l'obligation d'étudier de plus près la possibilité d'évolution.

En cas de solution future éventuelle au niveau international (voir à ce sujet le chapitre 11), il existerait de **nouvelles possibilités de blocage technique à la source** (p. ex.: les contenus racistes et extrémistes non punissables aux USA ne seraient plus visibles pour les Européens grâce à des dispositions techniques mises en œuvre par les fournisseurs d'hébergement).[29]

7. Acceptabilité et proportionnalité des blocages d'accès et des suppressions de contenus

Le caractère raisonnable ou déraisonnable d'une mesure est déterminé en partie par l'état de nécessité (art. 34 CP). Il est établi aussi par l'attitude de devoir vis-à-vis d'un

[29] Cette méthode a ainsi été utilisée jusqu'il y a peu pour empêcher les personnes qui ne sont pas citoyennes des USA de télécharger des navigateurs Internet sur les sites Web américains à l'aide d'un solide verrouillage.

délit commis par négligence[30], qui n'est plus pertinent en l'occurrence car un fournisseur de services Internet (que ce soit le fournisseur d'accès ou le fournisseur d'hébergement) qui a connaissance de contenus punissables et n'y réagit pas se comporte généralement de façon (éventuellement) intentionnelle[31].

Au sens d'un acte exécuté en état de nécessité, un tel comportement serait alors punissable si l'on ne pouvait exiger raisonnablement de l'ISP le sacrifice de son bien[32]. Le comportement raisonnable doit par conséquent être adapté aux circonstances, au sens de la pesée des biens juridiques opposés. Du fait que cette pondération des intérêts en conflit est exclusivement réservée aux tribunaux, il est impossible de fixer, dans le présent document, une règle générale permettant de déterminer à quel bien juridique il convient de donner la primauté, ce d'autant que ces biens [33] sont généralement difficiles à quantifier.

Pour ce qui est de l'acceptabilité dans une certaine mesure, il faut certainement tenir compte aussi des possibilités de contournement d'un blocage d'accès. Il convient néanmoins d'attirer l'attention sur le fait que la participation causale à un délit éventuellement réalisée par un fournisseur de services Internet suffit pour invoquer la complicité[34]. Quand bien même le blocage de l'accès ne peut pas être intégral pour les clients suisses par leur fournisseur ou si un contenu du fournisseur de contenu à effacer peut être placé sur le serveur d'un autre fournisseur d'hébergement, une telle procédure se justifie en principe même pour des quotas de réussite inférieurs à 100 % - à l'instar des missions de prévention de la police ou de la douane.

Ces développements valables pour ce qui concerne la complicité s'appliquent également par analogie à la responsabilité subsidiaire du fournisseur de services Internet conformément au droit pénal des médias, d'autant que la question de causalité ne se pose pas en raison du fait que l'art. 322bis CP vise un délit autonome.

---

[30] Voir Trechsel/Noll, CP AT I, 4e édition, Zurich 1994, p. 243
[31] Voir à ce sujet le résumé de l'avis de droit de l'OFJ sous le pt 8
[32] En premier lieu, son bien qui, d'une part, peut consister en un avantage de concurrence par un accès illimité et qui, d'autre part, peut être diminué par le recours nécessaire à des ressources techniques et humaines.
[33] Outre son bien, d'un côté, entrent en considération, de l'autre: la protection de la jeunesse et la protection de l'intégrité sexuelle conformément à l'art. 197 CP; le respect de la paix publique, de la dignité humaine ou de la protection du sentiment d'être respecté par les autres comme un autre en vertu de l'art. 261bis CP; le bien et le droit de disposer de soi-même pour les droits de propriété intellectuelle.
[34] Cf. ATF 120 IV 272 selon lequel "la complicité doit augmenter les chances de réussite d'un acte réunissant les éléments constitutifs d'une infraction"; ATF 119 IV 292: "Selon la jurisprudence, est réputée complicité toute contribution causale à l'acte, dans la mesure où cet acte se serait déroulé autrement sans l'aide du complice. Il n'est pas indispensable que l'acte n'aurait pas pu être réalisé sans la complicité."

Face à la situation légale et technique, les mesures suivantes doivent être considérées comme raisonnables [35] :

- **Si un fournisseur d'accès reçoit des autorités répressives des informations détaillées et concrètes sur des contenus qui présentent un caractère pénal, il veille au blocage de l'accès à ces sites** au sens des mesures répertoriées sous le point 6. Font partie de ces mesures: le blocage de l'adresse IP si le contenu punissable est stocké sur un **site ayant sa propre adresse IP,** ainsi que le blocage de l'URL incriminé dans le serveur proxy.

- **Si un fournisseur d'hébergement dispose d'informations concrètes et détaillées (ne provenant pas exclusivement d'autorités répressives) sur des contenus punissables se trouvant sur un de ses serveurs, il veille à ce que ces contenus ne soient plus accessibles ou soient effacés. Si ces renseignements n'émanent pas d'une autorité répressive, il doit lui même procéder aux recherches complémentaire nécessaires, au besoin en faisant appel à une autorité de poursuite pénale ou à des tiers professionnellement qualifiés. Le même principe s'applique s'il dispose d'informations obtenues grâce à ses relations contractuelles avec le fournisseur de contenu le faisant douter de la légalité de l'utilisation de la capacité mise à disposition**.

[35] Demeurent naturellement réservés le jugement par les tribunaux du caractère raisonnable (dans chaque cas d'espèce) et la question de savoir si un comportement punissable du fournisseur est donné .

8. Attitude exigée des fournisseurs sous l'angle de la responsabilité pénale

En guise de conclusion, l'attitude suivante est attendu des fournisseurs de services:

8.1. Fournisseurs d'accès:

- Si le fournisseur d'accès est en possession d'indices concrets émanant d'une autorité de poursuite pénale et liés à de présumés contenus illicites circulant sur le réseau, il est invité à procéder à des **blocages**, pour autant que ceux-ci soient raisonnables.
- **Il n'est pas concevable ni rationnel de rechercher activement et individuellement** des contenus répréhensibles sur Internet en raison du changement et de l'augmentation que subissent quotidiennement les données; une telle mesure ne peut donc être exigée.

8.2. Fournisseurs d'hébergement:

- Le fournisseur d'hébergement est tenu de rechercher des informations détaillées et concrètes liées à des **contenus du Web et à des groupes de discussion (newsgroups) illégaux.** S'il en trouve, ils doivent être **effacés** ou leur accès doit être **bloqué**.
- Etant donné que le fournisseur d'hébergement a des relations nettement plus étroites avec le fournisseur de contenu que le fournisseur d'accès, le fournisseur d'hébergement est tenu de **surveiller, du moins par sondage, les fournisseurs de contenus suspects**.
- En ce qui concerne les fichiers se trouvant sur des **serveurs FTP,** qui permettent le libre stockage des données, la surveillance est de mise pour autant que les fichiers puissent être lus par des logiciels de type classique.

8.3. Fournisseurs de services en ligne

- **Suivant l'organisation de leurs services,** les fournisseurs de services en ligne sont des **fournisseurs de contenu, d'hébergement ou d'accès.** La question de leur responsabilité pénale doit donc être envisagée selon leurs fonctions.

Pour tous les fournisseurs de services Internet, les points suivants s'appliquent:

- **Les dispositions mentionnées sous les points 8.1 à 8.3 se limitent aux services publics. Les services non publics, par contre, tombent sous le coup**

du secret des télécommunications. Aussi, ne peut-on attendre du fournisseur de services Internet qu'il ait connaissance du contenu ni qu'il prenne des dispositions à cet égard. Dès lors, une responsabilité pénale du fournisseur de services Internet peut par principe être exclue pour le domaine non public d'Internet.

- Le fournisseur de services Internet n'a **aucune obligation de dénoncer** des attitudes ou des contenus punissables vis-à-vis des autorités policières. Le **droit de dénonciation,** valable généralement, s'applique néanmoins. En cas de délit poursuivi sur plainte (p.ex. délits contre l'honneur, certaines infractions contre les droits d'auteur), soit le fournisseur de contenu peut être rendu attentif à la peine à laquelle il s'expose par son comportement, soit la personne concernée peut être informée de l'atteinte à ses droits.

- **En ce qui concerne les enquêtes pénales qui ne visent pas les fournisseurs, sont valables les devoirs généraux découlant du droit de procédure pénale appliqué (cantonal ou de la Confédération)**: devoir de déposer à titre de témoin, devoir de remettre des documents ou des informations prélevés dans des mémoires électroniques. En ce qui concerne les services protégés par le secret des télécommunications (e-mail, private-chat, téléphonie via Internet), les décisions des autorités compétentes selon la procédure pénale applicable[36] doivent être exécutées. Citons notamment:
  - **les renseignements sur le trafic Internet des utilisateurs clients du fournisseur de services Internet**[37]. Ces renseignements doivent autant que possible être fournis en temps réel, c'est-à-dire que, pour autant que la technique le permette, il s'agit de procéder à une surveillance directe[38]. L'autorité qui ordonne la surveillance (elle confie le soin d'exécuter la mesure au Service des tâches spéciales du DETEC[39]) doit dédommager le fournisseur de manière appropriée[40].
  - les données personnelles de chaque utilisateur relatives au trafic et à la facturation qui sont stockées dans les fichiers log. Ces données doivent pouvoir être mises à la disposition des autorités compétentes pendant au moins six mois[41].

- Les frais qui découlent des **mesures de blocage ou de suppression** se justifient en raison de la responsabilité pénale prévue dans le droit pénal des médias ou par la complicité possible avec l'infraction principale. Ces mesures représentent un comportement normal sous l'angle du droit pénal, lequel ne doit pas être dédommagé.

---

[36] en relation avec l'art. 44 LTC
[37] art. 44, al. 1, LTC
[38] art. 44, al. 2, LTC
[39] cf. ordonnance du 1er décembre 1997 sur le service de surveillance de la correspondance postale et des télécommunications (RS 780.11)
[40] cf. ordonnance du 12 décembre 1997 sur les émoluments et les indemnités en matière de surveillance la correspondance postale et des télécommunications (RS 780.115.1)
[41] (dans le cadre de la surveillance des télécommunications selon l'art. 44 LTC) art. 50 de l'ordonnance sur les services de télécommunications (OST; RS 784.101.1)

9. Attitude à attendre de la Confédération

- En cas de connaissance de contenus illicites, des dénonciations (contre les fournisseurs de contenu) seront d'abord déposées auprès des autorités compétentes au niveau cantonal, ou la présence de ces contenus sera communiquée aux autorités étrangères, pour que **l'infraction principale et les auteurs principaux** soient **poursuivis** en premier lieu.
- L'administration fédérale **apporte son soutien** - pour autant qu'elle dispose des connaissances spécialisées nécessaires - aux fournisseurs, qui doivent juger du caractère éventuellement répréhensible des contenus et mettre en œuvre de mesures de blocage de nature technique.

10. Autres angles d'action

Collaboration internationale renforcée
Outre le blocage, il existe d'autres possibilités - mais **plutôt efficaces à moyen terme** - de lutter contre les contenus illégaux sur Internet. C'est ainsi que la Police fédérale et d'autres offices ont intensifié leur collaboration avec des partenaires étrangers pour tendre à une convergence des points de vue et de la poursuite pénale en matière de contenus illicites sur Internet.

Unification du droit
Une harmonisation internationale des états de fait juridiques - un droit "(plus) compatible avec Internet" - serait certes souhaitable mais n'est pas prévue dans un avenir proche. Les Etats-Unis pourraient être un partenaire important quoiqu'ils favorisent ,involontairement, l'antisémitisme et le racisme à l'échelon international en hébergeant des sites Web extrémistes et racistes.

Accords internationaux sur les contenus illicites
Une solution réaliste consisterait à ratifier les accords internationaux concernant les contenus illicites diffusés sur Internet. Voici les **quelques ébauches** existant déjà:

- Conseil de l'Europe: Recommandation du Comité des Ministres du Conseil de l'Europe sur la criminalité en relation avec l'ordinateur (R (89) 9) et Recommandation relative aux problèmes de procédure pénale liée à la technologie de l'information (R (95) 13).[42] En 1997, un comité d'experts a été appelé à se pencher sur le thème du "crime in cyber-space" et devrait présenter fin 2000 un projet de convention internationale pour la lutte contre la criminalité sur Internet.[43]
- OCDE: Proposition française présentée à l'OCDE pour une Charte de coopération internationale sur Internet, qui pose également les principes d'une coopération en matière de poursuite pénale.[44]
- UE: plan d'action pluriannuel (1999-2002) de lutte contre les "messages à contenu illicite et préjudiciable diffusés sur les réseaux mondiaux" du 25.1.1999.[45] Le

[42] www.privacy.org/pi/agreements.html
[43] Les "terms of reference" qui ont depuis été prolongés de fin 1999 à fin 2000 peuvent être consultés sur le site Web du Conseil de l'Europe: http://www.coe.fr/cm/dec/1997/583/583.a13.html
[44] www.telecom.gouv.fr/francais/activ/techno/charteint.htm
[45] http://www.europa.eu.int/eur-lex/fr/lif/dat/1999/fr_399D0276.html

projet de l'UE se limite de prime abord à l'autoréglementation des fournisseurs (règles déontologiques) et aux mesures techniques combinables (outils de classement et de filtrage). Des mécanismes de "signalement" par ligne téléphonique directe devraient être prévus à l'échelon européen pour permettre aux utilisateurs de signaler des contenus qu'ils jugent illégaux.

- En novembre 1997, l'ONU a tenu à Genève un séminaire sur ce thème et a demandé à ses Etats membres d'adapter et d'harmoniser leurs législations nationales.
- La Commission des Communautés européennes a adopté le 18 novembre 1998 la proposition de directive du Parlement européen et du Conseil relative à certains aspects juridiques du commerce électronique dans le marché intérieur[46]. L'article 12, disposition particulièrement intéressante, dispose que la responsabilité du prestataire ne peut être engagée pour le "simple transport" (au sens du terme "accès" employé dans le présent avis). Aux termes de l'art. 13, ce principe vaut aussi pour la forme de stockage dit "caching". En ce qui concerne l'hébergement, l'art. 14 stipule que la responsabilité du fournisseur d'hébergement ne peut être engagée sauf s'il a effectivement connaissance de l'activité illégale de l'utilisateur. L'art. 15 ne prévoit, pour les fournisseurs de services visés aux art. 12 à 14, aucune obligation de surveillance sauf s'ils y sont invités par les autorités judiciaires[47]. Dans la position commune du Conseil du 28.2.2000 concernant cette proposition de directive, il a été précisé que la directive n'était pas destinée à harmoniser le domaine du droit pénal. En ce qui concerne les art. 12 à 14 de la proposition de directive, de nouveaux paragraphes 3 prévoient la possibilité de dispositions juridiques et administratives. Enfin, l'art. 15 de la directive n'empêche pas les Etats membres d'instaurer, pour les fournisseurs de services Internet[48], l'obligation de coopérer avec les autorités.
- Pour terminer, le Département fédéral des affaires étrangères a lancé l'idée d'une conférence internationale sur les contenus à caractère raciste diffusés sur Internet, lors de la conférence de Washington de novembre 1998 concernant les avoirs l'Holocauste. Il a reparlé de cette problématique dans le cadre de la Commission de l'ONU sur les droits de l'homme en mars 1999 et souhaite mettre sur pied, en collaboration avec d'autres Etats, une conférence internationale pour la lutte contre les sites Web à caractère raciste et antisémite. Les mesures de lutte élaborées à cette occasion devraient être approuvées lors de la conférence internationale contre le racisme prévue en 2001[49].

Collaboration plus étroite des fournisseurs, auto-contrôle

Une autre possibilité gage de succès en la matière consiste en une collaboration plus étroite des fournisseurs de services aux niveaux national et international. Ensemble, ceux-ci peuvent exercer une pression plus grande sur les fournisseurs d'autres pays pour les inciter à ne pas tolérer de tels contenus sur leurs serveurs même si la loi le permet théoriquement. **La base de cette collaboration serait constituée des différentes conditions générales et des codes de conduite des fournisseurs qui, à quelques exceptions près, refusent pour le moins les contenus à**

[46] Voir Ulrich Sieber, Verantwortlichkeit im Internet, p. 317 ss.
[47] Voir Ulrich Sieber, Verantwortlichkeit im Internet, p. 232 s.
[48] Voir la communication de la Commission du 29.2.2000 in PCE (2000) 386 définitif
[49] Voir à ce sujet un document rédigé pour une réunion de préparation à la conférence de 2001 à Genève: Rosenthal, David: Current Problems and Possible Strategies for Combating Racism on the Internet, janvier 2000 (http://www.rvo.ch/docs/unracism.pdf).

caractère raciste. L'expérience montre que les fournisseurs sont également disposés à réagir aux informations d'autres fournisseurs et de supprimer pareils contenus. De nombreux fournisseurs ont aussi installé une ligne téléphonique directe pour signaler l'existence de tels contenus; jusqu'à présent, ces lignes se limitent généralement à leurs propres serveurs. **Compte tenu de l'esprit de coopération qui caractérise les acteurs d'Internet, cette solution d'ordre général pourrait être intéressante et mener à un "Internet plus propre" grâce à un effort personnel**. On pourrait également s'inspirer de l'exemple de l'auto-contrôle introduit dans l'industrie des loisirs. La condition indispensable à cela serait l'acceptation d'une instance de jugement commune.

11. Et ensuite ?

Le groupe de contact ad hoc a demandé **une discussion approfondie au sujet des questions légales et techniques liées à la recommandation de blocage de la Police fédérale.** Le présent avis répond à cette exigence, même s'il subsiste certaines incertitudes imputables au développement sans précédent des technologies et au principe de l'indépendance fondamentale de la justice.

De plus, le groupe de contact a fait naître une meilleure prise de conscience en la matière tant au sein de l'administration fédérale que parmi les fournisseurs de services Internet.

En déterminant les conditions juridiques et techniques dans ce dossier, le groupe de contact a rempli son objectif initial.

La **nécessité d'une plate-forme de discussion commune et coordonnée** entre la Confédération et les fournisseurs de services Internet pourrait subsister à l'avenir et ce, indépendamment des recommandations de blocage de la Police fédérale. Voici ce que pourraient être les **besoins futurs** en matière **de coordination**:

- **coordination des indices concrets** émanant des autorités de poursuite pénale sur les contenus répréhensibles;
- harmonisation des **efforts** nationaux et internationaux **pour endiguer la criminalité sur Internet;**
- poursuite du **développement technique et juridique;**
- conseil et coordination des autorités cantonales de poursuite pénale dans **le traitement des dénonciations** sur des contenus illicites stockés à l'étranger;
- **unité de doctrine des autorités fédérales** face aux fournisseurs de services Internet;
- **interlocuteur unique** du côté des fournisseurs de services Internet;
- encouragement **à l'échange des connaissances et à la compréhension mutuelle.**

Il est possible de répondre diversement à ces besoins :

1. Abandon de la coordination

ex. parce que les besoins en matière de coordination ne sont pas considérés comme suffisamment patents pour justifier l'utilisation de ressources.

2. Chacun s'occupe de sa propre coordination

ex. parce que les intérêts de chaque groupe (fournisseurs de services Internet, autorités cantonales de poursuite pénale, administration fédérale) sont trop éloignés pour pouvoir mettre raisonnablement sur pied une plate-forme commune.

3. Création d'un organisme commun de coordination et d'information

ex. auprès d'un service privé indépendant de la Confédération et des fournisseurs de services Internet (organisation contre le racisme), ou à la Confédération (OFP, commission contre le racisme, DETEC, OFJ) ou auprès des fournisseurs (organisation centrale). Cette collaboration de la Confédération, des cantons et de l'économie privée devrait s'opérer de manière parfaitement transparente pour éviter toute accusation de censure.