Rapport à l'appui d'avant-projets de modification du code pénal suisse et du code pénal militaire

concernant

la responsabilité pénale des prestataires et les compétences de la Confédération relatives à la poursuite des infractions commises par le canal des médias électroniques (cybercriminalité)

Berne, octobre 2004

Condensé

L'évolution extrêmement rapide des techniques de l'information et de la communication, telles qu'Internet ou la téléphonie mobile, au cours des dernières années a modifié les habitudes de vie et de communication des individus comme nul autre facteur ne l'avait jamais fait auparavant. En effet, aujourd'hui, où que l'on soit dans le monde, on peut appeler des informations à partir de chaque raccordement au réseau. Néanmoins, bien qu'incontestés, les avantages offerts par les moyens de communication électroniques ont aussi un revers de la médaille car la « Toile » permet de commettre des infractions à partir de n'importe quel point du globe.

La « cybercriminalité » ne cesse de prendre de l'ampleur alors que le code pénal et le code pénal militaire ne permettent pas toujours de répondre de manière claire à certaines questions touchant la responsabilité pénale des divers prestataires de services qui participent à la commission de ces infractions. Il s'agit des fournisseurs de contenus, qui diffusent sur Internet leurs propres contenus ou des contenus repris de tiers ; des fournisseurs d'hébergement, qui mettent à la disposition de leurs clients - les fournisseurs de contenus - un espace sur lequel ces derniers peuvent offrir leurs propres contenus ; et enfin des fournisseurs d'accès qui permettent, d'un point de vue technique, aux utilisateurs d'accéder à Internet.

Par ailleurs, déployant ses effets au niveau planétaire, la cybercriminalité place les autorités de poursuite pénale devant de nouveaux défis. En effet, l'efficacité des interventions des autorités cantonales atteint rapidement ses limites face à la complexité des délits transfrontaliers commis par l'intermédiaire de réseaux de communication électroniques, les cyberdélits. On constate au niveau des cantons un manque de criminalistes spécialisés et un manque de moyens. Dans bien des cas, à l'ouverture d'une enquête, l'autorité cantonale compétente pour la poursuite n'est pas clairement définie. Si l'on veut gagner la lutte engagée contre cette forme moderne de criminalité, il est indispensable d'améliorer les modalités de la collaboration entre autorités fédérales et autorités cantonales.

Par la présente révision du code pénal et du code pénal militaire, le Conseil fédéral propose de préciser la réglementation légale de la responsabilité pénale des prestataires et de permettre, par l'amélioration des conditions-cadres dans la collaboration entre la Confédération et les cantons, une lutte plus efficace contre les délits commis sur les réseaux informatiques. La lutte contre la cybercriminalité figure d'ailleurs dans le Programme de la législature 2003 à 2007 en tant qu'objet des grandes lignes (FF 2004, 1035).

Afin de permettre une approche politique différenciée, le Conseil fédéral a élaboré un rapport contenant deux avant-projets. L'avant-projet A concerne la responsabilité pénale des prestataires, l'avant-projet B les compétences de la Confédération dans la poursuite des infractions commises sur les réseaux de communications électroniques.

1. Point de la situation

1.1 Commission d'experts « Cybercriminalité »

En été 1998, la Police fédérale constatait que divers sites Internet aux contenus racistes, qui avaient donné lieu, en Suisse, à des condamnations pour violation de l'article 261bis CP, continuaient d'être accessibles en ligne à tout un chacun. A la suite de cette constatation, la Police fédérale a envoyé aux fournisseurs de services Internet en Suisse une circulaire leur demandant de tester le blocage des sites incriminés. Cette circulaire déclencha un tollé parmi ces prestataires, réaction qui déboucha sur la mise sur pied d'un groupe de contact composé de représentants des services fédéraux concernés et des fournisseurs.

La question de la responsabilité pénale encourue par les prestataires pour les contenus illégaux véhiculés sur le réseau ayant prêté à controverse au sein du groupe de contact, l'Office fédéral de la justice (OFJ) fut chargé d'établir un avis de droit sur ce sujet. Dans son avis de droit du 24 décembre 1999[1], l'OFJ a conclu à une responsabilité subsidiaire du pur fournisseur d'accès au regard du droit pénal des médias, à condition que ce fournisseur ait été clairement rendu attentif à l'existence du contenu illégal par une autorité de poursuite pénale. L'OFJ précisait, en outre, que pour les cas dans lesquels le droit pénal des médias n'était pas applicable, les prestataires pouvaient être punis en qualité de complices de l'infraction principale.

La branche des prestataires rejeta les conclusions formulées dans l'avis de droit de l'OFJ et mandata les professeurs Niggli, Riklin et Stratenwerth, d'examiner à leur tour la question de la responsabilité pénale de ces mêmes prestataires. Dans leur avis daté d'octobre 2000[2], les trois experts sont parvenus à des conclusions contredisant, pour l'essentiel, celles de l'OFJ. En outre, ils ont souligné expressément le manque de clarté de la situation juridique et conclu à la nécessité de réviser le code pénal.

Le 14 décembre 2000, le conseiller aux Etats Thomas Pfisterer déposait une motion (00.3714)[3]. Cette motion avait pour objectif de prévenir les abus de l'Internet et de réglementer la cybercriminalité au plan du droit pénal. A cette fin, la motion requérait du Conseil fédéral une réglementation pénale - le cas échéant sous forme de dispositions isolées - satisfaisant aux critères de la sécurité juridique et de la praticabilité, et autant que possible coordonnée sur le plan international. Dans son développement, le motionnaire recommandait une harmonisation avec la Directive de l'Union européenne sur le commerce électronique[4] et présentait lui-même un projet de normes législatives. La motion Pfisterer fut adoptée par les deux conseils législatifs en 2001.

Compte tenu de ces développements, la cheffe du Département fédéral de justice et police (DFJP) d'alors a institué le 22 novembre 2001 une commission d'experts dont elle a confié la présidence à Peter Müller, alors sous-directeur de l'OFJ. Composée

[1] Publié in JAAC 64 75.
[2] Reproduit dans medialex, numéro spécial 1/2000.
[3] BO 2001, p. 27 s.
[4] Directive 2000/31/CE du Parlement européen et du Conseil de l'Union européenne du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique dans le marché intérieur (« Directive européenne sur le commerce électronique »).

de représentants de la doctrine, de la branche des prestataires et de l'administration fédérale, la commission avait pour mandat d'examiner quelles mesures peuvent être appliquées pour prévenir et sanctionner les infractions commises par le biais d'Internet. Dans ce cadre, elle était plus particulièrement chargée d'étudier le problème de la réglementation de la responsabilité pénale dans le domaine d'Internet. La commission d'experts « cybercriminalité » a remis son rapport en été 2003[5].

1.2 Groupe de travail « Genesis »

L'opération « Genesis », menée au cours de l'été 2002 pour lutter contre la pornographie enfantine sur Internet, était une opération nationale d'une ampleur jusqu'ici inégalée, associant presque tous les corps de police de Suisse ainsi que l'Office fédéral de la police (fedpol). Le nombre de procédures à engager en même temps et la dissémination des procédures sur l'ensemble du territoire national constituaient une nouveauté pour les autorités d'enquête suisses. Pour remédier à ces problèmes, la Police judiciaire fédérale (PJF) s'est chargée de la coordination de cette opération à l'échelon national, mais sans disposer des possibilités d'investigation requises au cours de la première phase de la procédure, jusqu'à la désignation des autorités cantonales compétentes de poursuite pénale, ni de la compétence de donner des instructions. La compétence en matière de poursuite pénale des infractions relevant de la pornographie (art. 197 CP) ressortit clairement aux cantons, qu'elles aient été commises à l'aide d'Internet ou d'autres moyens. Pour la première fois, l'opération « Genesis » a montré clairement que la collaboration entre la Confédération et les cantons requérait une révision du code pénal pour les cas soumis à la juridiction cantonale et concernant un grand nombre de personnes dans plusieurs cantons.

L'opération « Genesis » a suscité un intérêt marqué au sein de l'opinion publique et du monde politique, du reste déjà fortement sensibilisés aux questions de pornographie enfantine sur Internet et de criminalité sur Internet en général[6]. Le 26 septembre 2002, la conseillère nationale d'alors, Regine Aeppli Wartmann déposait une initiative parlementaire (02.452). Elle y demandait la création d'une compétence fédérale en matière de poursuite pénale des auteurs d'infractions relevant de la cybercriminalité, sur le modèle du Projet d'efficacité (art. 340bis CP)[7]. Le Conseil national a donné suite à cette initiative le 11 décembre 2003.

Compte tenu de ces développements, la cheffe du DFJP d'alors a demandé à fedpol l'automne 2002 une analyse relative au cadre juridique et organisationnel de l'opération « Genesis ». Cette analyse devait tirer les conséquences de l'opération pour les cas semblables à venir et présenter des propositions visant à améliorer la collabora-

[5] Rapport de la commission d'experts « Cybercriminalité », Département fédéral de justice et police, Berne, juin 2003.

[6] Cf. à ce propos les interventions parlementaires suivantes : Aeppli Wartmann Regine (01.3196), Améliorer la procédure de lutte contre la cybercriminalité; Motion Commission des affaires juridiques CN (01.3012), Lutte contre la pédophilie; Interpellation Tillmanns Pierre (00.3235), Lutte contre la pédophilie; Motion de la Commission 00.16-CN (00.3206), Grande criminalité. E-criminalité; Interpellation Freund Jakob (00.3059), Activités illégales sur Internet. Rôle de surveillance de la Confédération; Initiative cantonale Genève (00.314), Lutte contre la pédophilie; Motion von Felten Margrith (98.3467), Criminalité sur Internet. Responsabilité du fournisseur d'accès; Motion Jeanprêtre Francine (97.3487), Lutte contre la pornographie pédophile informatisée; Postulat Commission des affaires juridiques CN (96.3005), Pornographie enfantine sur Internet.

[7] BO 2003 N 1967.

tion entre la Confédération et les cantons. C'est ainsi que le groupe de travail « Genesis », composé de représentants des autorités judiciaires et policières, de la Conférence des commandants des polices cantonales de Suisse (CCPCS), de la Conférence des autorités de poursuite pénale de Suisse (CAPS) ainsi que d'autorités fédérales (fedpol, Ministère public de la Confédération et Office fédéral de la justice) a été mis sur pied. Ce groupe de travail a livré son rapport en novembre 2003[8].

Début 2003, soit environ six mois après le début de l'opération « Genesis », le Service de coordination de la lutte contre la criminalité sur Internet (SCOCI) a vu le jour. Rattaché à fedpol, ce service, financé par la Confédération et 25 cantons (tous hormis le canton de Zurich), soutient les autorités de poursuite pénale de la Confédération et des cantons en les aidant à détecter les actes punissables commis par le biais d'Internet (monitoring), en examinant les soupçons qui leur sont communiqués par des tiers pour ensuite les transmettre aux autorités de poursuite pénale compétentes (clearing) et en analysant le phénomène de la criminalité sur Internet. Les compétences d'enquête des autorités de poursuite pénale demeurent les mêmes malgré l'entrée en fonction du service de coordination. En d'autres termes, les investigations sont dans la plupart des cas du ressort des cantons. En outre, le SCOCI ne peut édicter des instructions destinées aux autorités de poursuite pénale compétentes**.**

[8] Rapport « Modèle de poursuite pénale pour les affaires intercantonales et internationales de cybercriminalité » du groupe de travail « Genesis », Berne, le 12 novembre 2003.

2. Responsabilité pénale des fournisseurs (Avant-projet A)

2.1 Commission d'experts « Cybercriminalité »

Dans son rapport, la commission d'experts établit que le droit pénal des médias, entré en vigueur le 1er avril 1998, n'est pas adapté à l'Internet[9]. Selon les dispositions du droit pénal des médias (art. 27, 27bis et 322bis CP), il faut que l'infraction ait été à la fois commise et consommée sous forme de publication pour tomber sous le coup desdites dispositions. En principe, seul l'auteur est punissable (art. 27, al. 1, CP). Si celui-ci ne peut être découvert ou s'il ne peut être traduit en Suisse devant un tribunal (art. 27, al. 2, CP), c'est le rédacteur responsable ou, à défaut, la personne responsable de la publication qui, en vertu de l'art. 322bis CP, encourt à titre subsidiaire une responsabilité pénale exclusive (la responsabilité en cascade). Le droit pénal des médias en vigueur est axé sur l'interaction de l'auteur, du rédacteur et des autres personnes responsables de la publication.

Cette réglementation n'est pas adaptée au cas du fournisseur d'hébergement qui se borne, en général, à mettre à la disposition de ses clients une infrastructure technique leur permettant d'offrir leurs propres sites et qui, partant, ne saurait être assimilé à la personne responsable d'une publication. Ce constat vaut également pour le fournisseur d'accès dont la prestation se limite à permettre aux utilisateurs finaux d'accéder à Internet.

De même, en ce qui concerne l'application des règles générales du CP concernant la qualité d'auteur de l'infraction et de participant, la commission d'experts a mis en évidence toute une série de questions qui se posent à propos tant du fournisseur d'hébergement que du fournisseur d'accès. Le fournisseur d'hébergement par exemple est qualifié soit d'auteur, soit seulement de complice de l'infraction en question selon la description de cet acte dans la norme pénale applicable. Mais, précisément dans le cas de la cybercriminalité et des éléments constitutifs qui la caractérisent, la frontière entre ces deux rôles est très floue. Ainsi, conformément à l'art. 197, ch. 1, CP, le seul fait de mettre des écrits pornographiques à la disposition de personnes de moins de seize ans suffit, ce qui ferait du fournisseur d'hébergement l'auteur de l'infraction. Or celui-ci se limite dans la majorité des cas à mettre à la disposition de son client (le fournisseur de contenu) une certaine capacité de mémoire sur son serveur. Il ne sait donc généralement pas quel genre d'informations son client a mis sur le réseau. Il ne peut savoir qu'il s'agit de contenus illicites que si des tiers l'en avertissent ou que s'il se livre lui-même à des contrôles préventifs.

Enfin, selon un arrêt rendu par le Tribunal fédéral en 1999[10], toute publication faite dans un média et consommée sous forme de publication ne constitue pas nécessairement un délit de média. Dans cet arrêt, le Tribunal fédéral considère explicitement que les représentations de la violence (art. 135 CP), la pornographie dure (art. 197, ch. 3, CP) et le négationnisme (notamment par le biais du « mensonge d'Auschwitz », art. 261bis, al. 4, CP) ne doivent pas être comptés parmi les délits de média. Pour l'essentiel, le Tribunal fédéral a avancé les arguments suivants à l'appui de sa décision : face à ce genre d'infractions, le législateur entendait empêcher la

[9] Rapport de la commission d'experts « Cybercriminalité », op. cit., p. 61 ss ; p. 68 s.
[10] ATF 125 IV 206 ss.

publication des contenus illégaux et ne voulait pas accorder à un groupe particulier de participants à l'infraction une position privilégiée en vertu du droit pénal des médias, art. 27 CP. Par ailleurs, il précisait qu'en matière de discrimination raciale, la Suisse était tenue, au niveau juridique international, par la ratification de la convention internationale contre la discrimination raciale[11], de poursuivre sans exception toute diffusion de déclaration raciste. Si cet arrêt a suscité de nombreuses critiques de la part d'auteurs de doctrine[12], la situation de confusion qui en est née tant du point de vue de la doctrine que de la jurisprudence a aussi mis en évidence l'impérieuse nécessité d'établir de nouvelles normes sanctionnant spécifiquement les infractions relevant de la cybercriminalité.

Le « noyau dur » du rapport de la commission d'experts est constitué par deux thématiques (elles sont traitées aux ch. 2.11 et 2.12 ci-dessous), à propos desquelles la commission a présenté un projet de normes rédigées; en outre, elle a formulé des suggestions touchant d'autres domaines du droit (cf. infra ch. 2.13).

2.11 La responsabilité pénale des prestataires

S'inspirant de dispositions arrêtées dans plusieurs pays étrangers afin de concrétiser la directive européenne sur le commerce électronique, la commission d'experts propose de compléter le code pénal par des normes réglant spécifiquement la responsabilité pénale des prestataires Internet (nouveaux art. 27 et 322bis AP-CP). En résumé, la réglementation proposée renferme le principe selon lequel les dispositions générales du CP relatives à la qualité d'auteur et de participant sont également applicables aux prestataires lorsqu'ils participent activement aux infractions. Le fournisseur n'est donc pas punissable si son action consiste uniquement à assurer l'accès automatisé à Internet, mais le devient s'il apprend ou constate ultérieurement qu'il met en circulation un contenu illégal et s'il omet de faire obstacle à l'utilisation de cette information[13].

2.12 Attribuer à la Confédération la compétence d'engager elle-même des poursuites pénales

Depuis le début de l'année 2003, la Confédération dispose d'un Service national de coordination de la lutte contre la criminalité sur Internet (SCOCI), service qui collabore avec les cantons (cf. supra ch. 1.2). En sus de cet instrument, la commission d'experts propose - selon le modèle figurant dans le projet dit « d'efficacité »[14], art.

---

[11] FF 1992 III 265 ss.

[12] Franz Riklin, Kaskadenhaftung – quo vadis? Medialex 2000, p. 208; Franz Riklin/Günter Stratenwerth, Medienstrafrecht/Kaskadenhaftung, in : Niggli/Riklin/Stratenwerth (édit.), Die strafrechtliche Verantwortlichkeit von Internet-Providern, medialex, édition spéciale 2000, p.13 ss.; Dorrit Schleiminger/Christoph Mettler, Strafbarkeit der Medienverantwortlichen im Falle der Rassendiskriminierung, art. 27, art. 261bis, al. 4, CP, remarques relatives à l'ATF 125 IV 206 ss, AJP 2000, p. 1039 ss; Jörg Rehberg/ Andreas Donatsch, Strafrecht, Verbrechenslehre, 7ème édition, Zurich 2001, p. 166; Christian Schwarzenegger, E-Commerce – Die strafrechtliche Dimension, in: Arter/Jörg (édit.), Internet-Recht und Electronic Commerce Law, Lachen et St-Gall 2001, p. 349 ss; Franz Riklin, Strafrecht, Allgemeiner Teil, 2ème édition, Zurich 2002, p. 245; Franz Zeller, in Niggli/Wiprächtiger, Basler Kommentar, StGB I, Bâle 2003, ad art. 27, n. 32.

[13] Rapport de la commission d'experts « Cybercriminalité », op. cit. , p. 93 ss.

[14] Le projet dit « d'efficacité » vise à améliorer l'efficacité et la légalité dans la poursuite pénale dans tous les cas dans lesquels les infractions ont été commises, pour une part prépondérante, à l'étranger

340bis CP - que la Confédération ait la compétence de poursuivre et de juger les auteurs des infractions commises par le canal des médias électroniques, en particulier lorsqu'elles concernent plusieurs cantons, sans qu'il y ait de prédominance évidente dans l'un d'entre eux, ou lorsque ces infractions nécessitent une procédure d'investigation coordonnée dans plusieurs cantons. En outre, le Ministère public de la Confédération doit pouvoir ouvrir une procédure d'investigation à la demande d'une autorité cantonale de poursuite pénale, soumettant ainsi l'affaire à la compétence juridictionnelle fédérale.

Cette proposition de la commission d'experts s'inspire de l'initiative parlementaire Aeppli Wartmann (cf. supra ch. 1.2).

2.13 Suggestions touchant d'autres domaines du droit

Pour la commission, il serait envisageable de prendre de nouvelles mesures de droit administratif qui, en complément des dispositions pénales, permettraient de prévenir les violations du droit sur les réseaux de communications électroniques. La commission relève toutefois que la plupart de ces mesures se heurteraient à des limites constitutionnelles, notamment à celles qui découlent des droits fondamentaux de la libre communication et du principe de la proportionnalité.

Par ailleurs, la commission d'experts estime souhaitable de clarifier sur le plan législatif certaines questions de la responsabilité civile qui se posent dans le contexte de la cybercriminalité.

Enfin, dans son rapport, la commission se penche sur les autres procédures législatives (alors) en cours dans le domaine de la cybercriminalité et émet diverses recommandations concernant ces procédures[15].

2.2 Avis et proposition du Conseil fédéral

Nul ne le contestera, l'évolution rapide des techniques de l'information et de la communication n'est pas sans influence sur la criminalité. D'une part, les nouvelles technologies facilitent la commission d'infractions « classiques » comme les atteintes à l'honneur, la pornographie ou la discrimination raciale. De l'autre, les techniques et les réseaux informatiques ouvrent la porte à de nouvelles formes de criminalité comme le vol de données ou la détérioration de données par la propagation de virus informatiques.

Conformément aux interventions parlementaires déjà mentionnées (notamment la motion Pfisterer et l'initiative parlementaire Aeppli Wartmann; cf. supra 1.1 et 1.2), le Conseil fédéral a placé la lutte contre la cybercriminalité et l'optimisation des poursuites pénales au Programme de la législature 2003 à 2007 en tant qu'objet des Grandes lignes. Le Conseil fédéral y prévoit de réglementer légalement la responsabilité

---

ou dans plusieurs cantons (FF 1998 1253 ss); modifications du code pénal en vigueur depuis le 1er janvier 2002 (RO 2001, 3071 3076).

[15] Rapport de la commission d'experts « Cybercriminalité », op. cit., p. 140 ss.

pénale des prestataires Internet et de doter les services fédéraux compétents de nouveaux pouvoirs d'investigation.

Ainsi qu'il est d'usage lors des révisions du code pénal ordinaire, le code pénal militaire doit être amendé en conséquence dans la mesure où les deux codes renferment la même norme.

2.21 Responsabilité pénale des prestataires

Le code pénal et le code pénal militaire en vigueur ne contiennent pas de dispositions sanctionnant explicitement la cybercriminalité. Eu égard au parallélisme[16] avec le droit pénal des médias, il convenait en premier lieu d'examiner si les éléments constitutifs de la cybercriminalité ne tombaient pas sous le coup des art. 27 et 322bis CP et 26a CPM ou s'il convenait de les apprécier en vertu des dispositions générales du code pénal et du code pénal militaire, notamment quant aux éléments constitutifs de la complicité (art. 25 CP ; art. 23 CPM).

Au terme d'une analyse approfondie des dispositions pénales en vigueur et compte tenu des avis de doctrine ainsi que de la jurisprudence du Tribunal fédéral, la commission d'experts « Cybercriminalité » a estimé que l'applicabilité du droit pénal des médias et des règles générales de participation du CP et du CPM était controversée et que de ce fait, dans la perspective de la sécurité du droit, une réglementation légale de ce domaine était également indiquée.

Le Conseil fédéral partage cette appréciation de la commission d'experts et propose de réglementer de manière explicite la responsabilité pénale des prestataires Internet dans le CP et le CPM.

La réglementation adoptée par la commission d'experts prévoit que les prestataires sont pénalement responsables quant aux contenus punissables circulant par le canal des médias électroniques, conformément aux dispositions générales du CP et du CPM applicables à la qualité d'auteur de l'infraction et de participant. Le fournisseur de contenus qui diffuse sur Internet des contenus illégaux, qu'il s'agisse de ses propres contenus ou de contenus repris de tiers, est punissable en qualité d'auteur des informations illégales. Le fournisseur d'accès est punissable en tant que co-auteur de l'infraction, complice ou instigateur lorsqu'il participe activement aux infractions commises par le fournisseur de contenus et ne se borne pas à assurer un accès automatisé à Internet. Est également punissable le fournisseur d'hébergement qui, par exemple, sait d'emblée que son client, le fournisseur de contenus, entend diffuser des informations punissables sur la capacité de mémoire qu'il met à sa disposition.

La réglementation proposée prévoit néanmoins les réserves suivantes à l'égard de la punissabilité des prestataires :

- Si le fournisseur de contenus est auteur ou rédacteur au sens du droit pénal des médias en vigueur, autrement dit s'il commet une infraction dans une publication en ligne, par exemple un quotidien publié sur Internet, c'est l'actuel art. 27 CP ou

[16] Les cyberdélits englobent également la publication (mise à disposition), la diffusion et la consommation (utilisation) d'informations. Une multitude de personnes participent du reste à la publication et la diffusion.

art. 26a CPM (nouvel art. 27bis AP-CP / nouvel art. 26b AP-CPM) qui est applicable.

- Le fournisseur d'hébergement n'est pas punissable s'il ignore, au moment où il met à la disposition du fournisseur de contenus une certaine capacité de mémoire, le genre d'informations que son client entend mettre sur le réseau. Mais s'il apprend ou constate ultérieurement que les données stockées sur son serveur constituent des informations punissables, et s'il omet d'en prévenir l'utilisation bien qu'on puisse techniquement et raisonnablement l'exiger de lui, le fournisseur d'hébergement est punissable. Il le sera également s'il omet de transmettre aux autorités de poursuite pénale les avertissements qui lui auront été adressés à ce propos par des tiers. Les fournisseurs de moteurs de recherche tels que google.com, altavista.com, etc. sont mis sur un pied d'égalité avec les fournisseurs d'hébergement.

- Le fournisseur d'accès dont la participation consiste uniquement à assurer l'accès automatisé à Internet n'est pas punissable. Cette impunissabilité du fournisseur d'accès est motivée par le fait que son action se limite à une transmission d'accès purement technique. De même, le stockage intermédiaire automatique et temporaire résultant de la consultation d'un utilisateur n'est pas punissable.

L'aspect déterminant de cette réglementation est le suivant : la punissabilité ou l'impunissabilité ne dépend pas uniquement du statut de prestataire de services Internet, mais de la fonction que celui-ci exerce à l'intérieur du processus de communication. Uniquement le fait d'être, par exemple, fournisseur d'accès ne constitue pas un motif absolu d'impunité.

La nouvelle réglementation s'appuie sur les dispositions en vigueur du CP et du CPM. Il va néanmoins de soi qu'après l'entrée en vigueur de la modification du CP (Dispositions générales, Entrée en vigueur et application du code) du 13 décembre 2002 (FF 2002 7658) et du CPM du 21 mars 2003 (FF 2003 2494), la numérotation des articles sera modifiée. Les propositions concernant les articles 27, 27bis et 27ter AP-CP deviendront les articles 28, 28a et 28b nCP, et les propositions concernant les articles 26a, 26b et 26c AP-CP deviendront les articles 27, 27a et 27b nCPM.

S'appuyant sur les résultats de la procédure de consultation relative à la nouvelle loi fédérale sur les loteries et les paris professionnels, dont la révision a été entre-temps suspendue, le Conseil fédéral est convaincu que la question de la responsabilité pénale des prestataires Internet doit être réglementée dans le CP et le CPM et non pas dans une autre loi fédérale. La disposition pénale prévue par le projet de révision de la loi sur les loteries, disposition qui aurait puni les prestataires Internet offrant des jeux non autorisés d'un an d'emprisonnement ou d'une amende allant jusqu'à un million de francs, dans les cas graves d'une peine de réclusion pouvant aller jusqu'à cinq ans ou d'une peine d'emprisonnement d'un an au moins, a été nettement rejeté par les participants à la consultation. Ces derniers ont relevé par contre qu'ils approuveraient une réglementation de la responsabilité pénale des fournisseurs Internet telle que la commission d'experts « Cybercriminalité » la propose dans le code pénal.

Par la présente révision du CP et du CPM, le Conseil fédéral préconise une réglementation différenciée tenant compte des particularités techniques d'Internet. Par

ailleurs, cette proposition de réglementation est inspirée des prescriptions similaires en vigueur dans d'autres pays étrangers, notamment dans les pays voisins de la Suisse. Parmi ces prescriptions, il convient de citer la directive européenne sur le commerce électronique dont l'objectif est de créer un cadre juridique pour assurer la libre circulation des services de la société de l'information. En résumé, la présente révision du CP et du CPM est, ainsi que le requiert la motion Pfisterer, une réglementation satisfaisant aux critères de la sécurité juridique et de la praticabilité, et harmonisée avec les droits des Etats voisins. Le présent projet visant à réglementer légalement la responsabilité pénale est en phase avec la diversité des fonctions assumées par le prestataire Internet.

2.22 Mesures d'accompagnement

En parallèle à cette réglementation pénale, le Conseil fédéral a également examiné les mesures d'accompagnement suivantes touchant le droit administratif et le droit civil.

2.221 Droit civil

Dans son rapport, la commission d'experts estime que le droit suisse en matière de responsabilité des fournisseurs d'accès et des fournisseurs d'hébergement est lacunaire et manque de clarté[17]. Elle en conclut la nécessité de légiférer dans le but de renforcer rapidement la sécurité du droit et suggère que cette réglementation légale se fasse dans le cadre soit de la loi fédérale sur le commerce électronique, soit de la loi fédérale sur la révision et l'unification du droit de la responsabilité civile (loi sur la responsabilité civile).

Le Conseil fédéral ne partage pas les appréciations de la commission d'experts en la matière. La réglementation de droit civil de la responsabilité des prestataires n'est ni lacunaire ni confuse. L'art. 50 du code des obligations (CO), selon lequel les instigateurs, les auteurs et les complices d'infractions répondent solidairement des dommages qu'ils ont causés, est à cet égard déterminant. Comme dans les autres cas de responsabilité éventuelle, il est laissé à la pratique le soin de juger des conditions à remplir concrètement pour qu'un prestataire soit considéré comme complice au sens de cette disposition. Il en va de même de l'appréciation des prétentions en cessation ou suppression du trouble à raison de la faute, notamment en cas d'appréciation d'une atteinte à la personnalité causée par un texte diffusé ou devant être diffusé sur Internet (art. 28 CC)

Contrairement au droit pénal, le droit civil des médias n'a pas fait l'objet, de par la volonté du législateur, de dispositions particulières. Comme la commission d'experts a dû elle-même le reconnaître, cette solution a fait ses preuves et n'a pas mené à des situations choquantes. Selon le Conseil fédéral, le législateur n'a pas besoin de fournir une contribution supplémentaire à la sécurité du droit ; la commission d'experts n'a donc pas fait de proposition concrète à ce sujet. Il en irait autrement si l'intérêt politique requerrait que l'on défende le comportement des prestataires dans

[17] Rapport de la commission d'experts « Cybercriminalité », op. cit., p. 86.

une mesure jusqu'ici ignorée. Cela n'est et ne doit pas être l'objectif d'un projet voué en premier lieu à la lutte contre la cybercriminalité.

Pour le reste, le Conseil fédéral rappelle que les travaux de révision du droit de la responsabilité civile ont été suspendus et que la future loi fédérale sur le commerce électronique traite essentiellement de la protection des consommateurs. Une réglementation de la responsabilité des prestataires ne pourrait donc pas se faire dans la loi fédérale sur le commerce électronique même si la nécessité de légiférer relevait du droit privé.

2.222 Droit administratif

Le Conseil fédéral partage les réflexions de la commission d'experts à propos des éventuelles mesures de droit administratif[18]. L'introduction d'instruments de droit administratif entrerait effectivement en conflit avec l'interdiction de la censure. En vertu de la liberté d'expression, on ne pourrait pas non plus imposer aux prestataires davantage d'obligations de droit administratif que celles qui découlent indirectement des propositions d'art. 27 et 322bis AP-CP et 26a AP-CPM. La réglementation proposée sanctionnera le fournisseur d'hébergement qui est « sûr » qu'un tiers commet une infraction par le biais de l'infrastructure qu'il met à sa disposition. Il n'est néanmoins pas tenu d'examiner constamment si un tiers commet des infractions.

2.223 Autres mesures législatives

Le Conseil fédéral partage aussi l'avis de la commission d'experts quant aux autres mesures législatives en matière de cybercriminalité : la convention du Conseil de l'Europe sur la cybercriminalité peut en effet devenir un instrument majeur dans la lutte contre cette forme de délinquance. La Suisse et l'entraide judiciaire internationale ont à cet égard tout intérêt à ce que le plus grand nombre possible de pays adoptent une norme identique. A cet effet, la convention devra être mise en œuvre dans un grand nombre de pays, ce qui n'est actuellement pas le cas du fait de la complexité de la thématique, de la nécessité d'interpréter le texte et du domaine d'application extrêmement large des dispositions de procédure. Par ailleurs, à moyen terme, la question d'une adaptation du droit suisse dépendra considérablement de la mesure dans laquelle il sera fait usage des possibilités de déclarations et de réserves à la convention. Dans tous les cas, ces démarches devront se faire en coordination avec les travaux d'unification de la procédure pénale suisse.

Toutefois, il n'est pas nécessaire de réviser la loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication (LSCPT)[19], ainsi que le requiert la commission d'experts dans son rapport[20]. En effet, conformément à la décision du 27 avril 2004 de la commission de recours du Département fédéral de l'environnement, des transports, de l'énergie et de la communication[21], le législateur

---

[18] Rapport de la commission d'experts « Cybercriminalité », op. cit., p. 79 ss.
[19] RS 780.1
[20] Rapport de la commission d'experts « Cybercriminalité », op. cit., p. 148 s.
[21] La décision de la commission de recours DETEC du 27.4.2004 peut être consultée (en allemand) à l'adresse Internet suivante :
http://www.reko-inum.admin.ch/de/display_file.php?fname=114010669724120&query= .

a établi avec l'art. 14, al. 4 LSCPT une norme spéciale prévoyant selon une procédure simplifiée, pour les infractions commises au moyen d'Internet, une obligation globale de renseigner dans le but d'identifier l'auteur de l'infraction. Cette obligation vaut même si les données sont couvertes par le secret des communications. Les demandes de renseignements au sens de l'art. 14, al. 4 LSCPT ne sont donc pas considérées comme mesures de surveillance si elles concernent une adresse IP dynamique et ont pour objet des données relatives aux communications ou permettant l'identification des participants. Conformément à son libellé, l'art. 14, al. 4 LSCPT entend donc obliger le prestataire Internet à fournir les renseignements demandés quant aux infractions commises par le canal d'Internet, indépendamment de la liste des actes punissables figurant à l'art. 3 LSCPT et de ne pas restreindre cette obligation de renseigner à certaines données.

2.3 Commentaires des dispositions proposées[22]

2.31 Code pénal

Ainsi que nous l'avons déjà mentionné, il existe un certain parallélisme entre la réglementation proposée et le droit pénal des médias. Néanmoins, les textes normatifs proposés ne sont pas le simple reflet des articles en vigueur 27 et 322bis CP et 26a CPM, cela à plusieurs égards : la nouvelle réglementation englobe tous les cyberdélits et n'est donc pas limitée, comme le droit pénal des médias, aux délits de médias. En droit pénal des médias, la responsabilité pénale du rédacteur responsable ou de la personne responsable de la publication n'entre en ligne de compte que si l'on ne peut découvrir l'auteur ou si l'auteur ne peut être traduit en Suisse devant un tribunal (responsabilité en cascade). Cette exclusion de la punissabilité n'existe pas pour les infractions commises par le canal des médias électroniques. Même si l'auteur ou le fournisseur de contenus sont connus ou peuvent être traduits devant un tribunal suisse, la punissabilité du fournisseur d'hébergement demeure, conformément à l'art. 322 ^{bis} AP-CP. En outre, dans le cas des cyberdélits et contrairement aux délits des médias (art. 322bis, phrase 2, CP), la négligence n'est pas punissable.

2.311 Adjonction apportée au titre marginal 6 dans le titre deuxième du CP

La commission d'experts propose de compléter le titre marginal sixième dans le titre deuxième du CP par les termes « sur les réseaux de communications électroniques ». La notion de « réseau de communications électroniques » est neutre du point de vue technologique et ne se rapporte pas uniquement au réseau Internet. Elle recouvre non seulement l'interconnexion d'ordinateurs, mais encore le recours à d'autres techniques de télécommunication. Des déclarations attentatoires à l'honneur par exemple ou des images pornographiques peuvent être diffusées via Internet (courrier électronique, WWW), mais aussi via un réseau de téléphonie mobile (SMS, MMS) ou encore sur le réseau local fermé d'une entreprise qui n'utilise pas forcément la technologie Internet. Peu importe également que les informations soient transmises sur des lignes ou par voie hertzienne ou encore que l'infrastructure de transmission soit constituée de lignes téléphoniques ou de conduites électriques. Par

[22] Pour plus de précisions, se reporter au rapport de la commission d'experts « Cybercriminalité », notamment p. 96 ss.

ailleurs, que les informations soient accessibles unilatéralement (par ex. dans le cadre des émissions traditionnelles de radio et de télévision) ou de manière interactive, c'est-à-dire dans le cadre de l'échange bilatéral de données (par ex. dans les conversations téléphoniques ou dans l'envoi et la réception de messages électroniques), ne joue aucun rôle.

L'expression « sur les réseaux de communications électroniques » est censée recouvrir tous les actes punissables en rapport avec la transmission, la préparation ou la mise à disposition d'informations sur les réseaux de télécommunications. Les délits de média classiques continueront, quant à eux, d'être soumis à l'actuel droit pénal des médias, qui sera intégré dans la nouvelle réglementation (art. 27bis et art. 322bis, ch. 2 AP-CP).

2.312 Responsabilité pénale des prestataires

Article 27 AP-CP Punissabilité sur les réseaux de communications électroniques

Nous l'avons dit, la notion de « réseaux de communications électroniques » a une portée plus large que celle de « médias ». Cela explique que la nouvelle norme consacrée aux infractions commises sur de tels réseaux figure au début de l'ensemble de la réglementation proposée et soit suivie de la disposition actuelle concernant les infractions commises dans les médias en tant qu'article 27bis AP-CP. Pour des raisons identiques, la même permutation a lieu à l'art. 322bis AP-CP, la norme qui figure actuellement dans cet article étant reprise en tant que chiffre 2. Quant à l'actuel art. 27bis CP (Protection des sources), il devient l'art. 27ter AP-CP.

Alinéa 1 Fournisseurs de contenus

L'al. 1 du nouvel art. 27 AP-CP statue que les règles générales du CP, et plus précisément celles qui ont trait à la qualité d'auteur et de co-auteur d'infractions, à la complicité et à l'instigation, sont applicables en premier lieu aux prestataires Internet. Ce principe vaut pour le fournisseur de contenus en tant qu'auteur des contenus illégaux. Il est également applicable aux fournisseurs d'accès et d'hébergement qui prennent une part active à la préparation ou à la mise à disposition d'informations illégales. La punissabilité ou l'impunissabilité du fournisseur ne dépend donc pas de son statut, mais de la fonction qu'il occupe dans le processus de communication. Ce principe est applicable sous réserve des dispositions suivantes des alinéas 2 à 4.

La « transmission », la « préparation » et la « mise à disposition » sont trois opérations fondamentales, spécifiques des réseaux de communications électroniques. On entend par transmission l'émission et la réception d'informations sur des lignes ou par des ondes hertziennes ; la préparation correspond au chargement d'informations sur un support de données public, accessible par le biais de réseaux de communications électroniques et, enfin, la mise à disposition est l'entretien d'un support de données public sur lequel des informations sont stockées. La dernière étape dans le processus de communication serait l'interrogation, en général le fait de l'utilisateur. Cette action n'est pas punissable. Par contre, depuis le 1er avril 2002, le stockage et le téléchargement de données aux contenus pornographiques sont punissables en vertu de l'art. 197, ch. 3bis CP.

La notion d' « informations » est très large puisqu'elle inclut aussi les programmes informatiques. Elle figure dans la loi sur les communications[23] tout comme dans la directive européenne sur le commerce électronique. La réglementation proposée ne se limite donc pas aux « délits d'expression » sur Internet, par exemple les représentations de la violence (art. 135 CP), la pornographie (art. 197 CP) ou la discrimination raciale (art. 261bis CP), mais va plus loin. Elle englobe aussi les autres domaines de la cybercriminalité tels que les indications visant la production de virus informatiques (art. 144bis CP), les offres frauduleuses sur la Toile (art. 146 CP) et les délits pénaux en matière de droit d'auteur (art. 67 et 69 de la loi sur les droits d'auteur, LDA[24]).

Alinéa 2 Délimitation des nouvelles normes par rapport au droit pénal des médias

Si le fournisseur de contenus est auteur ou rédacteur selon le droit pénal des médias (art. 27 CP et 27bis AP-CP), à savoir si une infraction est commise par la publication en ligne dans un média, par exemple dans un quotidien publié sur Internet, la réglementation prévue par l'art. 27bis AP-CP est applicable. Toutefois, la réserve ne mentionne que les auteurs et les rédacteurs et exclut les « personnes responsables de la publication en cause» dont l'actuel art. 27, al. 2 CP tient compte. Pour la raison suivante : dans le cas des infractions commises au travers des procédés automatisés sur les réseaux de communication électroniques, les fournisseurs d'accès et les fournisseurs d'hébergement responsables de la publication, à l'exception des auteurs et des rédacteurs, doivent tomber sous le coup de la nouvelle réglementation. C'est ce que doit garantir la restriction aux auteurs et rédacteurs de la réserve en faveur du droit pénal des médias.

Alinéa 3 Fournisseur d'hébergement

L'al. 3 établit une distinction entre le cas, le plus courant, du transfert automatisé des données, dont le fournisseur d'hébergement ignore le contenu, et le cas dans lequel il détecte ou apprend ultérieurement la punissabilité des contenus. Dans le premier cas, il n'est pas punissable ; dans le second par contre, il l'est conformément à l'art. 322bis, ch. 1 AP-CP.

De nombreux utilisateurs d'Internet commencent leurs recherches sur la « Toile » par le biais d'un moteur de recherche (par exemple, google.ch ou altavista.com). Du point de vue pénal, les exploitants de ces moteurs de recherche seront traités sur le même pied que les fournisseurs d'hébergement. Ce complément à l'al. 3, phrase 2 est nécessaire car les informations que contient l'index du moteur de recherche ne sont plus « d'autrui » au sens de la phrase 1. Ce n'est pas un quelconque fournisseur de contenus qui met ses informations à disposition sur le serveur de l'exploitant du moteur de recherche, mais l'exploitant du moteur de recherche lui-même qui établit une banque de données selon un procédé automatisé. Ce qui se trouve dans l'index constitue un contenu propre et devrait en conséquence être apprécié à la lumière de l'art. 27, ch. 1 AP-CP.

---

[23] Cf. à ce propos la définition légale figurant à l'art. 3, let. a de la loi du 30 avril 1997 sur les télécommunications (LTC; RS 784.10): "informations : les signes, signaux, caractères d'écriture, images, sons et représentations de tout autre type destinés aux êtres humains, aux autres êtres vivants ou aux machines.".

[24] RS 231.1

Alinéa 4 Fournisseur d'accès

Ainsi que nous l'avons mentionné et explicité, l'application des dispositions générales du CP n'exclut pas que le fournisseur d'accès soit sanctionné par exemple comme complice à l'infraction principale commise par le fournisseur de contenus. Mais en général, le fournisseur d'accès ne fait que permettre un accès à Internet. Lorsque la participation du fournisseur d'accès consiste uniquement à assurer l'accès de l'utilisateur à Internet, elle n'est pas punissable aux termes du ch. 4. L'utilisateur a recours aux différents services Internet pour communiquer ou pour obtenir des informations. Il a donc besoin d'un accès au réseau.

Conformément à cette disposition, le stockage automatique, temporaire et intermédiaire d'informations d'autrui doit aussi être compris comme fourniture d'accès. Contrairement à la directive européenne sur le commerce électronique[25], le Conseil fédéral propose de ne pas faire de distinction entre le stockage intermédiaire exigé par des impératifs techniques et la forme de stockage dite « *caching* », c'est-à-dire le stockage intermédiaire temporaire opéré par le fournisseur d'accès. Cette forme de stockage permet de rationaliser l'interrogation de données pour tous les clients du fournisseur d'accès, s'agissant de contenus souvent consultés. Cette solution flexible est préférable à une réglementation différenciée car une délimitation sous forme généralement abstraite n'est guère possible dans un environnement technique en constante mutation. Le « mode miroir » (*mirroring*), c'est-à-dire la copie d'un certain contenu Internet, résultant du comportement actif d'un prestataire sur un autre serveur, par exemple pour raccourcir les intervalles d'accès à un serveur particulièrement chargé, ne figure pas dans la réglementation proposée. Ne sont ici concernés que les cas de stockage intermédiaire automatique résultant de la consultation d'un utilisateur.

Article 27bis AP-CP Punissabilité des médias

L'art. 27bis AP-CP reprend la teneur de l'actuel art. 27 CP, seul le renvoi figurant à l'al. 2 étant modifié (art. 322bis, ch. 2 CP et non plus art. 322 CP).

Art. 322bis AP-CP Défaut d'opposition à une infraction commise sur les réseaux de communications électroniques et dans les médias

Ch. 1, al. 1

L'al. 1 régit la punissabilité du fournisseur d'hébergement, telle qu'elle est statuée au nouvel art. 27, al. 3 AP-CP. La nouvelle norme en question sanctionne un délit véritablement spécial dont l'auteur ne peut qu'être que celui qui met à disposition selon un procédé automatisé, sur un réseau de communications électroniques, des informations d'autrui. Cette disposition vise les fournisseurs d'hébergement sur les serveurs desquels les clients, autrement dit les fournisseurs de contenus, mettent en ligne leurs informations, sans que les premiers puissent exercer une quelconque influence sur la teneur de ces informations.

[25] Cf. art.12, al. 2 et art. 13 de la convention européenne sur le commerce électronique.

Le ch. 1, al. 1 consacre véritablement la punissabilité de l'omission : il est fait grief au fournisseur d'hébergement de ne pas être intervenu – bien que l'on pût techniquement et raisonnablement l'exiger de lui – pour empêcher l'utilisation d'un fichier dont il est sûr qu'il présente, par exemple, des contenus racistes ou pornographiques ou encore qu'il fait l'apologie de la violence. Ce n'est pas la participation au délit principal, mais l'inaction face à la propagation de l'information illégale qui constitue le noyau proprement dit de l'acte illicite.

La disposition requiert que l'infraction ait été commise au moyen d'informations d'autrui. Les infractions visées ici peuvent être réparties en deux catégories: d'une part, les infractions traditionnellement associés à la cybercriminalité, telles que les représentations de la violence (art. 135 CP), la pornographie (art. 197 CP) ou la discrimination raciale (art. 261bis CP) ; d'autre part toutes les infractions pour la commission desquelles le recours à des moyens de communications électroniques est envisageable tels que les délits informatiques, mais aussi les infractions classiques contre le patrimoine (p. ex. l'escroquerie ; art. 146 CP) et les infractions sanctionnées par le droit pénal accessoire, notamment celles qui ont un rapport avec la concurrence déloyale ou violent le droit d'auteur ou le droit des marques.

Ch. 1, al. 2

Le ch. 1, al. 1 CP requiert une connaissance sûre permettant de fonder la punissabilité de l'omission commise par le fournisseur d'hébergement. Cela pose la question de savoir ce qu'il doit advenir du fournisseur d'hébergement qui n'a pas obtenu cette connaissance sûre, par exemple parce que les informations qui lui sont parvenues sont lacunaires. Si le fournisseur d'hébergement reste passif, il ne pourra jamais obtenir la connaissance requise au regard de l'al. 1 et demeurait alors non punissable. C'est ce qu'entend éviter le nouvel al. 2. La punissabilité du fournisseur d'hébergement est aussi donnée en vertu de l'al. 2 lorsque ce fournisseur omet de porter à la connaissance des autorités de poursuite pénale les avertissements reçus de tiers quant à des informations constituant une infraction. L'important à cet égard est que cette obligation de transmission soit créée uniquement par des communications adressées individuellement au fournisseur d'hébergement, et non par des informations généralement accessibles au public, émanant par exemple de la presse écrite, de la radio ou de la télévision.

En outre, le fournisseur d'hébergement doit répercuter uniquement les informations concernant des fichiers qu'il héberge lui-même. Cette obligation de transmission ne touche donc que le fournisseur d'hébergement qui ne peut obtenir cette connaissance sûre et demeure passif malgré des avertissements incomplets ou lacunaires. Dans ce sens, il ne s'agit pas d'un devoir général de dénoncer, même si un fournisseur d'hébergement prudent transmet aux autorités de poursuite pénale tous les avertissements qui lui sont communiqués.

Ainsi, grâce aux alinéas 1 et 2, l'objectif politico-juridique visant à impliquer les fournisseurs d'hébergement dans la lutte contre les contenus illicites sur Internet est également atteint. On ne peut leur demander d'empêcher totalement les infractions que leurs clients, à savoir les fournisseurs de contenus, commettent en publiant leurs fichiers sur le serveur des hébergeurs ; ceux-ci n'ont, en effet, aucune espèce d'influence sur le processus de mise en ligne des contenus concrets. Néanmoins, on peut très bien les exhorter - et c'est justement là le véritable objectif de la loi - à limi-

ter ces infractions dans leurs répercussions, en rendant impossible la prise de connaissance des contenus en question. Ils peuvent par exemple en entraver l'utilisation technique ou transmettre les avertissements qui leur parviennent aux autorités de poursuite pénale en vertu de l'al. 2.

Tant l'al. 1 que l'al. 2 prévoient une peine d'emprisonnement (de trois jours à trois ans ; art. 36 CP) ou une amende (jusqu'à 40 000 francs ; art. 48 CP)[26]. Cette quotité de peine apparaît équitable si l'on considère les infractions principales qui sont également sanctionnées par une peine d'emprisonnement ou une amende (cf. art. 135, 197 et 261bis CP). Elle se justifie également eu égard à l'objectif politique visant à impliquer le fournisseur d'hébergement dans la lutte contre les contenus illicites : l'hébergeur limite les répercussions de l'infraction de son client, le fournisseur de contenus, en empêchant que l'utilisateur prenne connaissance du contenu illégal incriminé.

Ch. 1, al. 3

S'agissant des infractions commises sur Internet, qui sont poursuivies sur plainte, l'al. 3 propose que ces infractions ne soient poursuivies que si plainte a été effectivement déposée. Si tel n'est pas le cas, aucune procédure pénale ne sera ouverte à l'encontre du fournisseur d'hébergement. Une réglementation analogue a été adoptée pour le recel (art. 160 CP). Lorsque le fournisseur d'hébergement est averti d'un contenu constituant une infraction poursuivie sur plainte, bien souvent il ne sait pas si une plainte a été effectivement déposée. Aussi, dans le doute, répercutera-t-il l'avertissement sans se préoccuper de ce qu'il y ait eu plainte ou non. L'al. 3 vise à obvier à la situation paradoxale et choquante dans laquelle le fournisseur d'hébergement serait sanctionné selon l'al. 2 pour avoir omis de répercuter l'avertissement aux autorités de poursuite pénale, quand bien même la personne présumée lésée par l'infraction ne veut pas que l'on poursuive ni ne punisse son auteur.

Ch. 1, al. 4

En vertu de quel droit doit-on décider s'il y a infraction ? Le nouvel al. 4 apporte une réponse claire à cette interrogation : « La question de savoir si une infraction au sens des al. 1 et 2 peut être commise au moyen d'une information doit être appréciée en vertu droit suisse ». Cette disposition permet d'obliger le fournisseur d'hébergement à répondre pénalement de ses actes, même lorsque ceux-ci ne sont pas punissables au lieu de leur commission.

Dans ce contexte, cet alinéa pourrait revêtir une certaine portée pratique dans le cas de délits d'expression qui ne sont, par exemple, pas punissables selon le droit anglo-américain ou australien en raison de la liberté d'opinion telle qu'elle est conçue dans ces Etats, mais sont considérés comme racistes et discriminatoires selon le droit suisse. La punissabilité des fournisseurs d'hébergement, telle qu'elle est prévue aux al. 1 et 2, vise à empêcher que l'information tombant sous le coup du droit pénal

[26] Lors de l'entrée en vigueur de la modification du CP (Dispositions générales, Entrée en vigueur et application du code pénal) du 13 décembre 2002 (FF 2002 7658), l'expression « Emprisonnement ou amende » sera remplacée par « Peine privative de liberté jusqu'à trois ans ou peine pécuniaire ». La peine pécuniaire étant désormais établie selon un système de jour-amende, son montant maximal atteindra donc 1 080 000 francs (360 jours-amende à 3000 francs ; cf. art. 34 nCP).

puisse continuer à être consultée à partir d'un serveur installé en Suisse. Toutefois, un blocage ne peut revêtir un intérêt que si le fichier concerné contient des informations punissables selon le droit suisse.

Ch. 1, al. 5

Conformément à l'al. 5, les informations au sens des al. 1 et 2, à savoir celles au travers desquelles une infraction a été commise, doivent être supprimées. Comme la confiscation (art. 58 CP), dont elle constitue le pendant, la suppression de l'information est de nature matérielle. Elle est ordonnée dans le jugement du tribunal. L'al. 5 ne consacre pas une disposition de procédure analogue au séquestre qui permettrait aux autorités de poursuite pénale de bloquer provisoirement l'information. Celle-ci est réservée à la législation procédurale. Il s'agit ici en premier lieu d'une ordonnance de blocage; elle doit s'appuyer - en tant que mesure de contrainte - sur les dispositions correspondantes.

Une fois supprimés, les contenus illégaux ne doivent plus pouvoir être reconstitués. Ainsi que nous l'avons déjà mentionné, la suppression des informations est ordonnée par le tribunal lorsqu'il y a condamnation du fournisseur d'hébergement. Selon la commission d'experts, en cas d'acquittement ou en cas de liquidation procédurale d'une cause, il convient d'examiner comme suit dans quelle mesure une suppression entre également en considération : si l'on ne peut condamner un fournisseur d'hébergement, notamment parce que l'on ne peut prouver qu'il a eu une connaissance sûre de la punissabilité de l'information, mais que l'on peut prouver tout au plus un dol éventuel, le tribunal peut malgré tout ordonner la suppression des informations. En outre, la suppression des informations a lieu « que la Suisse ait ou non une compétence juridictionnelle ». Sous l'angle politico-juridique, il ne serait pas satisfaisant que le jugement d'acquittement prononcé à l'égard du fournisseur d'hébergement constate qu'un fournisseur de contenus a chargé un fichier constitutif d'infraction et contraire au droit sur le serveur du premier, mais qu'un effacement est néanmoins impossible parce que la Suisse n'a pas de compétence pour juger l'acte du fournisseur de contenus. Que la Suisse ait ou non une compétence juridictionnelle sur l'acte du fournisseur de contenus ne tire pas à conséquence en ce qui concerne la suppression des informations. Même si cette compétence n'existe pas, les informations sont supprimées du serveur Internet du fournisseur d'hébergement.

Ch. 2

Le ch. 2 reprend la teneur de l'actuel art. 322bis CP, seul le renvoi (art. 27bis et non plus art. 27 CP) étant modifié.

2.32 Code pénal militaire

Comme de coutume lors des révisions du code pénal ordinaire, le code pénal militaire doit également être modifié dans la mesure où la même prescription se trouve dans les deux textes législatifs (cf. infra ch. 2.42).

2.4 Avant-projet A

2.41 Code pénal suisse

(nouveau titre) 6. Punissabilité sur les réseaux de communications électroniques et dans les médias[27]

Art. 27 AP-CP
Punissabilité sur les réseaux de communications électroniques[28]

[1] Lorsqu'une infraction aura été commise par voie de transmission, de préparation ou de mise à disposition d'informations sur un réseau de communications électroniques, les dispositions générales du présent code relatives à la qualité d'auteur et de participant sont applicables. Les dispositions suivantes sont réservées :

[2] Lorsque l'auteur de l'infraction est auteur ou rédacteur au sens de l'art. 27bis, sa punissabilité est régie par cette disposition.

[3] La personne qui aura mis à disposition, selon un procédé automatisé, des informations d'autrui sur un réseau de communications électroniques sera punissable aux conditions prévues à l'art. 322bis, ch. 1. La mise à disposition d'un répertoire intégrant des informations d'autrui selon un procédé automatisé est considérée comme mise à disposition d'informations d'autrui.

[4] Celui qui se borne à fournir l'accès à un réseau de communications électroniques n'est pas punissable. Le stockage automatique et temporaire d'informations d'autrui suite à la consultation d'un site est considéré comme une fourniture d'accès.

L'art. 27 devient l'art. 27bis AP-CP ***Punissabilité des médias[29]***

[1] …

[2] Si l'auteur ne peut être découvert ou qu'il ne peut être traduit en Suisse devant un tribunal, le rédacteur responsable est punissable en vertu de l'art. 322bis, ch. 2. A défaut de rédacteur, la personne responsable de la publication en cause est punissable en vertu de ce même art., ch. 2.

[3] …

[4] …

[27] Lors de l'entrée en vigueur de la modification du CP (Dispositions générales, Entrée en vigueur et application du code pénal) du 13 décembre 2002 (FF 2002 7658), le Titre 6^{e} « Punissabilité sur les réseaux de communications électroniques et dans les médias » remplacera le Titre 6^{e} « Punissabilité des médias».
[28] Lors de l'entrée en vigueur de la modification du CP (Dispositions générales, Entrée en vigueur et application du code pénal) du 13 décembre 2002 (FF 2002 7658), l'art. 27 deviendra l'art. 28.
[29] Lors de l'entrée en vigueur de la modification du CP (Dispositions générales, Entrée en vigueur et application du code pénal) du 13 décembre 2002 (FF 2002 7658), l'art. 27bis deviendra l'art. 28a.

L'art. 27bis CP inchangé devient l'art. 27ter AP-CP
***Protection des sources*[30]**

Art. 322bis AP- CP
Défaut d'opposition à une infraction sur les réseaux de communications électroniques et dans les médias

1. Celui qui aura mis à disposition, selon un procédé automatisé, sur un réseau de communications électroniques, des informations d'autrui dont il est sûr qu'elles constituent une infraction et qui aura omis d'en prévenir l'utilisation, bien qu'on puisse techniquement et raisonnablement l'exiger de lui, sera puni de l'emprisonnement ou de l'amende[31].

Celui qui aura mis à disposition, selon un procédé automatisé, sur un réseau de communications électroniques, des informations d'autrui constituant une infraction et qui aura omis de transmettre aux autorités de poursuite pénale les avertissements qui lui ont été adressés par des tiers et lui sont effectivement parvenus, sera puni de l'emprisonnement ou de l'amende.

Si l'infraction est poursuivie sur plainte, l'acte ne sera poursuivi que si cette plainte a été effectivement déposée.

La question de savoir si une infraction peut être commise au moyen d'une information doit être appréciée en vertu du droit suisse.

Les informations au sens des al. 1 et 2 seront supprimées, que la Suisse ait ou non une compétence juridictionnelle.

2. La personne responsable au sens de l'art. 27bis, al. 2 et 3, d'une publication constituant une infraction sera punie de l'emprisonnement ou de l'amende si intentionnellement, elle ne s'est pas opposée à la publication. Si elle a agi par négligence, la peine sera les arrêts ou l'amende.

[30] Lors de l'entrée en vigueur de la modification du CP (Dispositions générales, Entrée en vigueur et application du code pénal) du 13 décembre 2002 (FF 2002 7658), l'art. 27a devient l'art. 28b

[31] Lors de l'entrée en vigueur de la modification du CP (Dispositions générales, Entrée en vigueur et application du code pénal) du 13 décembre 2002 (FF 2002 7658), l'expression « Emprisonnement ou amende » sera remplacée par « Peine privative de liberté jusqu'à trois ans ou peine pécuniaire ». La peine pécuniaire étant désormais établie selon un système de jour-amende, son montant maximal atteindra donc 1 080 000 francs (360 jours-amende à 3000 francs ; cf. art. 34 nCP).

2.42 Code pénal militaire

(nouveau titre) 8. Punissabilité sur les réseaux de communications électroniques et dans les médias[32]

Art. 26a AP-CPM
Punissabilité sur les réseaux de communications électroniques[33]

1 Lorsqu'une infraction aura été commise par voie de transmission, de préparation ou de mise à disposition d'informations sur un réseau de communications électroniques, les dispositions générales du présent code relatives à la qualité d'auteur de l'infraction et de participant sont applicables. Les dispositions suivantes sont réservées :

2 Lorsque l'auteur de l'infraction est auteur ou rédacteur au sens de l'art. 26b, sa punissabilité est régie par cette disposition.

3 La personne qui aura mis à disposition, selon un procédé automatisé, des informations d'autrui sur un réseau de communications électroniques sera punissable aux conditions prévues à l'art. 322bis, ch. 1 du code pénal. La mise à disposition d'un répertoire intégrant des informations d'autrui selon un procédé automatisé est considérée comme mise à disposition d'informations d'autrui.

4 Celui qui se borne à fournir l'accès à un réseau de communications électroniques n'est pas punissable. Le stockage automatique et temporaire d'informations d'autrui suite à la consultation d'un site est considéré comme une fourniture d'accès.

L'art. 26a CPM devient l'art. 26b AP-CPM
Punissabilité des médias[34]

1 …

2 Si l'auteur ne peut être découvert ou qu'il ne peut être traduit en Suisse devant un tribunal, le rédacteur responsable est punissable en vertu de l'art. 322bis, ch. 2 du code pénal. A défaut de rédacteur, la personne responsable de la publication en cause est punissable en vertu de ce même art., ch. 2 du code pénal.

3 …
4 …

L'art. 26b CPM inchangé devient l'art. 26c AP-CPM
***Protection* des sources[35]**

[32] Lors de l'entrée en vigueur de la modification du CPM (Dispositions générales, Entrée en vigueur et application du code pénal militaire) du 21 mars 2003 (FF 2003 2494), le Titre huitième « Punissabilité sur les réseaux de communications électroniques et dans les médias » remplacera le Titre sixième « Punissabilité des médias».
[33] Lors de l'entrée en vigueur de la modification du CPM (Dispositions générales, Entrée en vigueur et application du code pénal militaire) du 21 mars 2003 (FF 2003 2494), l'art. 26a deviendra l'art. 27.
[34] Lors de l'entrée en vigueur de la modification du CPM (Dispositions générales, Entrée en vigueur et application du code pénal) du 21 mars 2003 (FF 2003 2494), l'art. 26b deviendra l'art. 27a.

3. Compétences de la Confédération dans les cas d'infractions commises sur les réseaux de communi cations électroniques (avant-projet B)

3.1 Propositions du groupe de travail « Genesis »

Le groupe de travail « Genesis » s'est essentiellement penché sur des propositions d'amélioration d'ordre juridique, dans les domaines où l'analyse de l'opération avait permis de cibler des lacunes. Ces améliorations devraient permettre d'accroître l'efficacité de la poursuite pénale des auteurs d'infractions relevant de la cybercriminalité.

3.11 Poursuite pénale des auteurs d'infractions commises sur les réseaux de communications électroniques

Dans son rapport[36], le groupe de travail « Genesis » a clairement montré pourquoi les investigations touchant la cybercriminalité constituent un défi de taille, pour le personnel qui les effectuent, d'une part, et sur le plan technique, de l'autre. Les difficultés sont nombreuses. Mentionnons à titre d'exemple la saisie des moyens de preuve, qui requiert des effectifs et des moyens techniques considérables car dans ce monde virtuel des réseaux de communications électroniques, les coupables ont toute facilité pour demeurer anonymes ou pour effacer les traces de l'infraction commise. En outre, il s'agit généralement de cas complexes, présentant des liens avec l'étranger et pouvant selon les circonstances se répartir sur plusieurs cantons, comme dans le cas de l'opération « Genesis ». Enfin, l'équipement technique et la formation continue des enquêteurs sont très coûteux.

3.12 Analyse de l'opération « Genesis »

L'opération « Genesis » a mis en évidence la problématique spécifique de la lutte contre la cybercriminalité. De plus, le volume des moyens de preuve saisis et le fait que 25 cantons (tous sauf le canton d'Appenzell Rhodes-Intérieures) soient impliqués - chacun d'entre eux étant compétent en matière de poursuite pénale - ont placé les autorités d'enquête suisses face à une situation totalement nouvelle.

Dans son analyse, le groupe de travail « Genesis » a souligné la nécessité d'agir au niveau de la coopération entre la Confédération et les cantons, plus particulièrement dans les domaines de la préparation d'autres opérations du type « Genesis », de l'évaluation technique des preuves, de la formation des enquêteurs et de l'information aux médias. D'autres lacunes graves ont été mises en évidence. Ainsi, la Confédération n'a pas eu la possibilité par exemple de recueillir, auprès des entreprises de cartes de crédit, les données des clients impliqués. Si tel avait été le cas, les autorités fédérales auraient pu, dans le cadre de l'opération « Genesis », établir plus rapidement les compétences cantonales et transmettre plus rapidement aux

---

[35] Lors de l'entrée en vigueur de la révision du 21 mars 2003 de la partie générale du CPM (FF 2003 2494), l'art. 26c deviendra l'art. 27b.

[36] Rapport du groupe de travail « Genesis », op. cit., p. 34 s.

cantons concernés les affaires qui leur revenaient. Enfin, en raison de l'absence de base légale, la Confédération n'a pu exercer aucune influence sur le planning des enquêtes des 25 cantons impliqués, ce qui a rendu la tâche de coordination de fedpol particulièrement difficile.

Ces deux dernières lacunes, qui ont sérieusement entamé l'efficacité de l'opération, ont été constatées au cours de la première phase de la procédure. La poursuite des auteurs d'infractions commises à l'aide d'Internet relève en grande partie de la juridiction cantonale[37] et, dans ces affaires, la Confédération ne peut que coordonner les investigations menées aux échelons intercantonal ou international[38]. Dans l'état actuel du droit, les autorités fédérales ne sont donc aucunement habilitées à procéder elles-mêmes à des investigations ou à enjoindre aux cantons d'y procéder.

Les ressources disponibles sont toutefois insuffisantes pour lutter efficacement contre la cybercriminalité car les moyens de communications électroniques servent de plus en plus à commettre des infractions, un nombre croissant de personnes y ont accès et peuvent en utiliser toutes les possibilités techniques. De plus, de nombreuses autres grandes affaires laissent entrevoir, pour l'avenir, une multiplication probable des cas concernant plusieurs cantons, du type de ceux visés par l'opération « Genesis ». Pour cette raison, le groupe de travail « Genesis » a souligné dans son rapport[39] qu'il serait donc opportun et urgent d'octroyer à la Confédération la compétence de mener des investigations dans la première phase de la procédure pénale.

3.13 Pas de compétence fédérale permettant de poursuivre les auteurs d'infractions relevant de la cybercriminalité

Le groupe de travail « Genesis »estime néanmoins qu'il ne faut pas centraliser au niveau fédéral la poursuite pénale des délits commis sur les réseaux, ainsi que le suggèrent l'initiative parlementaire Aeppli Wartmann (cf. supra ch. 1.2) et la commission d'experts « Cybercriminalité » (cf. supra ch. 2.12).

Cette proposition va trop loin et n'est pas justifiée sur le plan matériel[40]. Le groupe de travail considère en effet que la répartition des tâches en matière de poursuite pénale qui est consacrée par la Constitution (la compétence cantonale constitue la règle, la compétence fédérale constitue l'exception) serait remise en question car les cantons devraient céder une part non négligeable de leurs prérogatives à la Confédération. L'analyse de l'opération « Genesis » a par ailleurs permis de déterminer que les problèmes principaux se situaient dans la première phase de la procédure, si bien qu'il ne paraît pas nécessaire que la Confédération mène la procédure du début à la fin[41].

---

[37] Cf. art. 343 CP.
[38] Cf. art. 2, let. b, de la loi fédérale du 7 octobre 1994 sur les Offices centraux de police criminelle de la Confédération (LOC1; RS 360) et art. 3 de l'ordonnance du 30 novembre 2001 concernant l'exécution de tâches de police judiciaire au sein de l'Office fédéral de la police (RS 360.1).
[39] Rapport du groupe de travail « Genesis », op. cit., p. 5 ss.
[40] Rapport du groupe de travail « Genesis », op. cit., p. 7 ss.
[41] Rapport du groupe de travail « Genesis », op. cit., p. 26 s.

3.14 Modèle proposé

Se fondant sur la législation en vigueur en matière de stupéfiants[42], le groupe de travail « Genesis » a élaboré un modèle qui permettrait de confier des pouvoirs d'investigation à la Confédération durant la première phase de la procédure, sans porter atteinte aux compétences des cantons en matière de poursuite pénale. Pour concrétiser ce modèle, deux variantes ont été mises au point (cf. ch. 3.15 et 3.16)[43]; elles reposent toutes deux sur l'introduction d'une nouvelle disposition dans le code pénal, les autorités de poursuite pénale fédérales disposant ainsi d'un instrument leur permettant de mener des investigations qui puisse être utilisé à moindre coût, d'une manière rapide, tout en respectant le principe de la proportionnalité.

3.15 Variante 1 (compétence d'enquête du Ministère public de la Confédération en vertu de l'art. 259 de la loi fédérale du 15 juin 1934 sur la procédure pénale [PPF][44], fondée sur la haute surveillance de la Confédération)

Ainsi que nous l'avons déjà mentionné, cette variante s'inspire de la loi sur les stupéfiants (art. 29, al. 4 LStup, en relation avec l'art. 259 PPF). Ses lignes de force sont les suivantes:

Le Ministère public de la Confédération peut, en vertu de l'art. 259 PPF, ordonner des recherches, si les actes punissables – comme lors de l'opération « Genesis » – ont été commis totalement ou partiellement à l'étranger ou dans plus d'un canton. Pour que l'art. 259 PPF puisse s'appliquer, la Confédération doit toutefois disposer d'un droit de haute surveillance sur la poursuite des auteurs des actes punissables concernés. Etant donné que la Confédération est dépourvue d'un droit de haute surveillance aussi bien dans le domaine spécifique de la pornographie (art. 197 CP) que dans celui de la cybercriminalité, un tel droit devrait être instauré.

Il est ainsi proposé de créer un art. 343bis AP-CP, établissant un droit de haute surveillance sur la poursuite des auteurs d'actes punissables commis sur les réseaux de communications électroniques.

L'instauration de cette haute surveillance de la Confédération serait possible tout en conservant l'application de l'art. 258 PPF en plus de l'art. 259 PPF. En vertu de cette nouvelle disposition, la Confédération aurait en outre la possibilité d'édicter des instructions à l'égard des autorités cantonales de poursuite pénale et, ainsi, de les obliger à instruire et exécuter une procédure.

3.16 Variante 2 (Compétence d'investigation des autorités fédérales)

La variante 2 proposée par le groupe de travail « Genesis » renonce à introduire un droit général de haute surveillance dans le domaine spécifique de la cybercriminalité de la Confédération ; elle poursuit néanmoins le même objectif que la variante 1.

---

[42] Loi fédérale du 3 octobre 1951 sur les stupéfiants et les puissances psychotropes (loi sur les stupéfiants, LStup); RS 812.121
[43] Rapport du groupe de travail « Genesis », op. cit., p. 9 ss et 22 ss.
[44] RS 312.0

Les autorités fédérales compétentes doivent, dans les cas d'infractions relevant de la cybercriminalité commises entièrement ou partiellement à l'étranger ou dans plus d'un canton, ordonner quelques recherches nécessitant des investigations urgentes, sans pour autant fonder une compétence juridictionnelle de la Confédération. Selon cette variante, la Confédération pourrait aussi édicter des instructions contraignantes à l'attention des cantons dans le cadre de la coordination des enquêtes impliquant plusieurs cantons et/ou un ou plusieurs Etats étrangers.

Il est proposé, à cet effet, de créer un art. 343bis AP-CP qui fonde pour l'autorité fédérale compétente la possibilité d'ordonner des recherches et d'édicter des instructions.

3.17 Mesures d'accompagnement

Le groupe de travail « Genesis » recommande en outre à titre de mesure d'accompagnement de compléter la loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication (LSCPT)[45]. Ce complément permettrait d'obliger les prestataires Internet de fournir des renseignements sur certaines données relatives aux communications, et ce même en dehors d'une procédure pénale formelle. Cette mesure permettrait d'attribuer de manière rapide les affaires aux autorités de poursuite pénale cantonales compétentes[46].

3.2 Avis et proposition du Conseil fédéral

L'opération « Genesis » a incontestablement souligné la nécessité de réglementer la collaboration entre la Confédération et les cantons dans les cas où un grand nombre de personnes et de cantons étaient impliqués. Le problème concret qui s'est posé pour la Confédération à propos de « Genesis » était l'absence de compétences au cours de la première phase de la procédure. C'est en effet durant cette phase qu'il s'agit d'identifier les personnes avant de transmettre l'affaire aux autorités cantonales compétentes en matière de poursuite pénale, de relever et de saisir les preuves et, d'une manière générale, de préparer les cas. Par ailleurs, du fait de cette absence de compétence d'instruction, il avait été impossible d'introduire simultanément les investigations. Le public avait été informé à différents moments. Ayant été ainsi prévenues, quelques-unes parmi les personnes visées avaient été en mesure d'éliminer des preuves déterminantes.

Nous l'avons déjà mentionné (cf. supra ch. 2.2), le Conseil fédéral a placé la lutte contre la cybercriminalité et l'optimisation des poursuites pénales au Programme de la législature 2003 à 2007 en tant qu'objet des Grandes lignes.

3.21 Pas de compétence fédérale permettant de poursuivre les auteurs d'infractions relevant de la cybercriminalité

Le Conseil fédéral a examiné les deux propositions qui lui ont été soumises : *compétence fédérale* par la commission d'experts « Cybercriminalité » (cf. supra ch. 2.12)

[45] RS 780.1.
[46] Rapport du groupe de travail « Genesis », op. cit., p. 29 s.

et *compétence d'enquête de la Confédération au cours de la première phase de la procédure*, conformément aux propositions du groupe de travail « Genesis » (cf. supra ch. 3.14 à 3.16). Il rejette l'instauration d'une compétence de la Confédération au sens d'une compétence juridictionnelle fédérale, cela pour les raisons suivantes :

Le Conseil fédéral considère en effet que la répartition des tâches en matière de poursuite pénale qui est consacrée par la Constitution (la compétence cantonale constitue la règle, la compétence fédérale constitue l'exception) serait remise en question car les cantons devraient céder une part non négligeable de leurs prérogatives à la Confédération, ce qui pourrait nécessiter une modification constitutionnelle. S'agissant par exemple de la pornographie, les cantons seraient compétents en cas de diffusion par le biais du cinéma ou dans les médias écrits et la Confédération en cas de diffusion par les réseaux de communications électroniques. Le Conseil fédéral estime qu'il convient d'éviter une telle source d'inefficacité dans les poursuites pénales. En outre, dans ce genre d'enquêtes, le travail classique de la police (auditions, séquestres, etc.), dans lequel les cantons ont plus d'expérience, prend par la suite une importance prépondérante. Les autorités d'enquête de la Confédération se verraient ainsi obligées, même dans le cadre de grandes opérations, de recourir à l'appui des cantons (ressources humaines et moyens logistiques), ce qui entraînerait pour eux une charge disproportionnée dans un domaine où ils ne sont plus compétents. L'analyse de l'opération « Genesis » a par ailleurs permis de déterminer que les problèmes principaux se situaient dans la première phase de la procédure, si bien qu'il ne paraît pas nécessaire que la Confédération mène la procédure du début à la fin. La mise en œuvre d'une compétence fédérale pour tenir compte des profondes modifications apportées au système de poursuite pénale prendrait beaucoup de temps et nécessiterait une réorganisation des domaines concernés au sein de la Confédération. La Confédération devrait également renforcer considérablement ses effectifs et débloquer des moyens financiers à hauteur de ceux qui ont été affectés au Projet d'efficacité, ce qui ne saurait se justifier eu égard à la précarité actuelle des finances fédérales.

3.22 Compétences d'enquête des autorités fédérales

A l'instar du groupe de travail « Genesis », le Conseil fédéral estime que le système actuel des poursuites pénales présente une lacune que l'attribution d'une compétence d'enquête aux autorités fédérales au cours de la première phase de la procédure est à même de combler.

Le Conseil fédéral a examiné de près les deux variantes proposées par le groupe de travail « Genesis » (cf. ch. 3.15 et 3.16) :

Si elles poursuivent toutes deux le même but - à savoir attribuer à la Confédération des compétences lui permettant de mener des investigations et de donner des instructions, notamment dans les cas impliquant un grand nombre de personnes et souvent plusieurs cantons -, ces deux variantes empruntent néanmoins des voies différentes :
La *variante 1* donne à la Confédération un *droit de haute surveillance* inspiré de la législation en vigueur en matière de stupéfiants (LStup). Toutefois, dans la LStup, la haute surveillance de la Confédération porte sur l'ensemble de la loi, et pas seulement sur les dispositions pénales. Une haute surveillance qui se limite uniquement à

la poursuite de certaines infractions réprimées par le CP, comme le propose le groupe de travail « Genesis », serait tout à fait nouvelle. Elle serait au demeurant assez floue. Le Conseil fédéral reconnaît que les autorités de poursuite pénale connaissent les procédures en raison de l'application qui en est faite dans la LStup et que ces procédures sont éprouvées. Mais il relève aussi les différences avec la cybercriminalité, domaine dans lequel la haute surveillance s'appliquerait à un nombre indéterminé de dispositions pénales du CP et du droit pénal accessoire. Pour toutes ces raisons, le Conseil fédéral rejette cette variante.

La *variante 2* du groupe de travail « Genesis » emprunte pour sa part une voie plus directe pour parvenir au même but. Les nouvelles compétences de la Confédération sont inscrites dans le CP directement et de manière exhaustive. Le texte de la variante 2[47] ne répond néanmoins pas entièrement aux critères de clarté et de précision requis par le CP, du point de vue stylistique et quant au contenu. Une telle formulation peut être source d'incertitudes pour les autorités chargées d'appliquer le droit. Par ailleurs, l'expression « … ou dans plusieurs cantons … » exclurait tous les cas impliquant plusieurs suspects, mais un seul canton. De même le cas contraire, un suspect mais plusieurs cantons, ne tomberait pas sous le coup de la norme telle qu'elle est formulée dans la variante 2. Cette réglementation serait donc peu judicieuse.

S'appuyant sur cette variante 2, le Conseil fédéral propose un nouvel article 344 AP-CP (cf. infra ch. 3.3) en vertu duquel le Ministère public de la Confédération (MPC) et la Police judiciaire fédérale (PJF) pourraient procéder aux premières investigations urgentes lorsqu'une infraction soumise à la compétence juridictionnelle des cantons a été commise par le canal des médias électroniques et que le canton compétent n'est pas encore établi. Cette compétence d'investigation du MPC et de la PJF au cours de la première phase de la procédure ne fonde pas de compétence juridictionnelle de la Confédération (cf. infra ch. 3.4). En outre, la Police judiciaire fédérale peut coordonner l'exécution des investigations par le moyen d'instructions.

Même si cette proposition n'élargit que modérément les compétences d'investigation de la Confédération, sa mise en œuvre requiert des moyens en termes de finances et de personnel. Selon une première estimation, il faudrait créer treize postes de travail supplémentaires. Cette estimation repose, il convient de le souligner, sur des données rassemblées dans le cadre de la coordination des procédures concernant la pornographie enfantine. Les ressources des autorités d'enquête devront toutefois être adaptées au potentiel croissant de délits dans ce domaine.

Le Conseil fédéral est conscient que les compétences de la Confédération ici proposées relèvent de la compétence juridictionnelle des cantons. Il conviendrait, en fait, de les réglementer juridiquement dans le nouveau code suisse de procédure pénale unifié. Mais ce dernier n'entrera probablement en vigueur que dans plusieurs années et, face à la nécessité de légiférer dans le domaine de la cybercriminalité, un complément du CP apparaît préférable et plus rapidement réalisable.

De l'avis du Conseil fédéral, la proposition d'article 344 AP-CP constitue une réglementation nécessaire et adéquate. Elle permettra d'améliorer la collaboration entre

[47] Rapport du groupe de travail « Genesis », op. cit., p. 22.

Confédération et cantons, contribuant ainsi à accroître l'efficacité de la poursuite pénale des infractions relevant de la cybercriminalité.

3.23 Mesures d'accompagnement

Pour les raisons déjà mentionnées (cf. supra ch. 2.223), le Conseil fédéral n'estime pas nécessaire de compléter la LSCPT[48] ainsi que le recommande le groupe de travail « Genesis » (cf. supra ch. 3.17).

3.3 Commentaires de l'art. 344 AP-CP (Compétences de la Confédération dans les cas d'infractions commises sur les réseaux de communications électroniques)

L'article proposé 344 AP-CP tient compte des particularités de la poursuite pénale dans les cas relevant de la cybercriminalité. Ces cas sont certes soumis à la compétence juridictionnelle des cantons, mais les informations dont disposent les autorités fédérales (Ministère public de la Confédération et Police judiciaire fédérale) ne leur permettent pas encore de savoir à quel canton attribuer la poursuite pénale. Il peut également y avoir des cas dans lesquels les autorités fédérales reçoivent des informations de l'étranger indiquant qu'un grand nombre de personnes dans plusieurs cantons sont soupçonnées d'avoir commis une infraction. On peut aussi envisager le cas où l'information vient de Suisse et où les autorités de poursuite pénale d'un seul canton sont compétentes, mais ne sont pas encore connues à ce stade de la procédure. Comme l'a clairement montré le groupe de travail « Genesis » dans son analyse, il est inutile dans ce genre de cas de transmettre ces informations telles quelles à tous les cantons pour que chacun de son côté procède aux mêmes investigations, entre autres afin de déterminer s'il a la compétence d'engager la poursuite pénale. Le véritable problème se situe à ce stade des enquêtes préliminaires.

3.31 Classement systématique et titre marginal du nouvel art. 344 AP-CP

Le classement systématique en tant que nouvel art. 344 AP-CP, accompagné du chiffre marginal 3, en conformité avec l'actuel art. 343 CP qui porte le titre marginal « 2. Juridiction cantonale » a pour but de souligner que cette norme ne créera par de nouvelle compétence juridictionnelle de la Confédération. Afin d'éliminer toute incertitude à ce sujet, cette volonté est de nouveau expressément précisée à l'al. 1 par la formulation « … infraction soumise à la compétence juridictionnelle des cantons … ». Le terme de « compétences » dans le titre marginal attire l'attention sur le fait qu'il ne s'agit pas seulement de compétences d'enquêtes ou d'investigations, mais comme l'al. 2 de l'art. 344 AP-CP l'établit expressément, également de compétences de coordination et de compétences d'édicter des instructions.

[48] RS 780.1

3.32 Alinéa 1

Le nouvel art. 344 AP-CP s'appliquera aux cas que l'on qualifie de complexes, d'une part parce que l'information provenant de Suisse ou de l'étranger concerne des infractions commises par un grand nombre de personnes dans plusieurs cantons, de l'autre parce que dans ce monde virtuel des médias électroniques, il convient d'appliquer d'autres méthodes d'investigation que dans le monde réel, méthodes qui sont par ailleurs en constante mutation du fait des progrès de la technique. Cela étant, ce nouvel article est formulé de manière si générale que les autorités pénales de la Confédération peuvent ouvrir une enquête dans tous les cas, soumis à la compétence juridictionnelle des cantons, d'infraction commise par le canal d'un média électronique. Le MPC et la PJF ont besoin d'une compétence légale afin de pouvoir exécuter les premières investigations nécessaires. Le droit actuel ne leur donne pas cette compétence. Ces investigations doivent être menées par le MPC et par la PJF conformément aux art. 100 ss de la loi fédérale du 15 juin 1934 sur la procédure pénale (Procédure pénale fédérale, PPF). Le MPC dirige les recherches de la police judiciaire (art.15/17 PPF). La PJF assume la tâche principale consacrée dans le nouvel article, à savoir le contact avec les cantons ainsi que l'analyse et la préparation des informations reçues. Au cours de cette première phase, durant laquelle la procédure est menée par la Confédération, la police cantonale assume une partie de la tâche de police judiciaire de la Confédération en ce sens qu'elle participe aux premières investigations (art. 17 PPF). Au terme des premières investigations urgentes, le MPC transmet le dossier à la police cantonale conformément à l'art. 107 PPF.

La notion de « premières investigations urgentes » recouvre à la fois les enquêtes visant à déterminer l'autorité cantonale de poursuite pénale compétente et toutes les mesures urgentes de conservation des preuves. L'expérience a montré qu'il s'agit essentiellement d'investigations ou enquêtes de nature technique visant à identifier des titulaires de cartes de crédit auprès des banques ou des instituts de crédit, ainsi que des suspects possédant une adresse électronique, auprès cette fois des prestataires suisses. Le progrès technique étant en constante évolution, les mesures ici énumérées ne peuvent être considérées comme exhaustives.

3.33 Alinéa 2

L'al. 2 attribue à la PJF un droit direct d'édicter des instructions à l'adresse des autorités cantonales de poursuite pénale pour ce qui est des procédures au sens de l'al. 1. Cette disposition a pour but de garantir que les investigations seront menées simultanément de même que l'information au public. Cela afin d'éviter, comme cela a été le cas dans l'opération « Genesis », que certaines personnes soient averties et fassent disparaître des preuves précieuses.

Les instructions mentionnées à l'al. 2 sont spécifiques. Il ne s'agit pas des instructions générales et usuelles servant de moyen de surveillance. Elles ne sont pas adressées aux gouvernements cantonaux, mais aux autorités cantonales de poursuite pénale. Contrairement aux instructions générales, ces instructions établies par les autorités fédérales à l'intention de certaines autorités cantonales ne sont pas utilisées dans le but de faire appliquer le droit fédéral, par exemple sous forme de circulaires adressées aux cantons, car elles constituent une atteinte à la compétence juridictionnelle du canton concerné. Mais dans la mesure où un tel pouvoir de donner

des instructions s'avère nécessaire pour des motifs matériels, il doit toujours se concrétiser au niveau d'un texte légal, cela dans toute la mesure du possible. C'est la raison pour laquelle l'al. 2 établit cette compétence.

Eu égard à la notion même d'instruction et à l'absence de possibilités d'exécution, l'adjectif « contraignantes » figurant dans la variante 2 du groupe de travail « Genesis »[49] est inutile. Une instruction est par essence contraignante, sinon elle serait une recommandation.

[49] Rapport du groupe de travail « Genesis », op. cit., p. 22.

3.4 Code pénal militaire

Il ne s’impose pas de réglementer de manière analogue l’avant-projet B du fait que les cas spécifiquement militaires sont difficilement concevables dans ce domaine. Par ailleurs, le CPM prévoit de remettre le traitement de tels cas aux autorités civiles (cf. 221 CPM).

3.5 Avant-projet B Code pénal suisse

Article 344 AP-CP

3. Compétences de la Confédération dans les cas d'infractions commises sur les réseaux de communications électroniques

[1] Si l'on soupçonne qu'une infraction soumise à la compétence juridictionnelle des cantons a été commise sur les réseaux de communications électroniques et si le canton compétent n'est pas encore établi, le Ministère public de la Confédération et la Police judiciaire fédérale peuvent procéder aux premières investigations urgentes. Ils appliquent à cet égard la loi fédérale du 15 juin 1934 sur la procédure pénale.

[2] La Police judiciaire fédérale peut coordonner l'exécution des investigations par le moyen d'instructions à l'attention des autorités cantonales de poursuite pénale.