



Le Forum des droits
sur l'internet

RECOMMANDATION

Les Enfants du Net - II
Pédo-pornographie et pédophilie
sur l'internet

Janvier 2005

SOMMAIRE

INTRODUCTION	5
I. LA DIFFUSION ET LE RECEL DE PEDO-PORNOGRAPHIE SUR L'INTERNET.....	7
1. <i>Evaluation générale du phénomène</i>	7
a. Un phénomène d'importance observé sur la plupart des protocoles de l'internet.....	7
b. Les serveurs d'images pédo-pornographiques sur le web concentrés géographiquement. 12	
c. Faut-il craindre que l'internet banalise la pédo-pornographie ?	13
2. <i>Etat des moyens en vue de combattre la diffusion et le recel de pornographie enfantine sur l'internet, et des limites de ces moyens.....</i>	14
a. Analyse des dispositifs pénaux réprimant le recel et la diffusion de pornographie enfantine.	14
b. Organisation et moyens des services d'enquête en France.....	20
c. Moyens et limites de la coopération policière et judiciaire internationale.	25
d. Analyse des responsabilités, obligations et initiatives des fournisseurs d'accès et de services en ligne.	31
II. L'UTILISATION DE L'INTERNET AUX FINS DE PREPARER UNE ATTEINTE SEXUELLE SUR UN MINEUR	37
1. <i>Perceptions et réalités des risques associés à certains usages de l'internet.</i>	37
a. Un objet d'inquiétude mal connu.....	37
b. Les usages sociaux de l'internet et leurs risques.	39
c. La question de la diffusion de données personnelles d'enfants.....	42
d. La relative ignorance des parents.....	43
2. <i>L'action des parties concernées et ses limites.</i>	43
a. Le cadre juridique et procédural en France et à l'étranger.	43
b. Rappel des responsabilités et initiatives des fournisseurs de services.	46
c. Initiatives publiques et privées de sensibilisation des jeunes utilisateurs de l'internet, des éducateurs et des familles.....	48
d. La contribution des logiciels de contrôle parental.	52
III.RECOMMANDATIONS.....	53
MIEUX CONNAITRE LES USAGES ET LES RISQUES	53
1. <i>Etudier les comportements des jeunes utilisateurs de l'internet et la diversité des risques auxquels ils peuvent être exposés sur le réseau.....</i>	53
2. <i>Recueillir et exploiter les statistiques policières et judiciaires pour mieux connaître les phénomènes.....</i>	55
3. <i>Organiser un rendez-vous annuel des acteurs de la protection des mineurs sur l'internet.</i>	55
SENSIBILISER LES JEUNES INTERNAUTES ET LES ADULTES	56
4. <i>Mettre en œuvre une vaste campagne de sensibilisation du grand public.....</i>	56
5. <i>Mobiliser tous les canaux publics au profit d'une information complète des jeunes internauts et de leurs parents.</i>	57
6. <i>Pour une éducation à des usages maîtrisés de l'internet à l'école.</i>	57
7. <i>Mobiliser les parents avec le soutien des associations familiales.....</i>	58
8. <i>Encourager fournisseurs d'accès et exploitants de services à adopter un standard élevé d'information des usagers de leurs services.</i>	58
DEVELOPPER LES OUTILS FAVORISANT LA MAITRISE DES USAGES DE L'INTERNET	59
9. <i>Renforcer les outils à la disposition des jeunes utilisateurs d'espaces interactifs et de logiciels de messagerie instantanée.</i>	59
10. <i>Renforcer la maîtrise de la diffusion de données personnelles relatives à des mineurs sur l'internet.....</i>	60
11. <i>Donner aux parents les moyens de choisir les meilleurs outils permettant de renforcer la sécurité des jeunes utilisateurs.</i>	61
ENGAGER UNE REFLEXION SPECIFIQUE SUR LE DROIT ET L'ORGANISATION DU DISPOSITIF REPRESSIF	62
12. <i>Approfondir la réflexion sur d'éventuelles évolutions du droit.</i>	62
13. <i>Adapter l'organisation des services d'enquête.....</i>	63
14. <i>Former enquêteurs et magistrats aux techniques et aux procédures de la recherche d'infractions sur l'internet et les supports informatiques.</i>	64

15. Clarifier le dispositif encadrant la conservation des données de connexion.....	64
RENFORCER LA COOPERATION INTERNATIONALE POLICIERE ET JUDICIAIRE.....	65
16. Mettre en œuvre et promouvoir les dispositions de la Convention sur la cybercriminalité en matière de lutte contre la pédo-pornographie.....	65
17. Renforcer la coopération, l'entraide judiciaire et les échanges de bonnes pratiques au sein de l'Union européenne.....	65
CONCLUSION : POURSUIVRE LA REFLEXION SUR LES RESEAUX MOBILES ET LES NOUVEAUX SUPPORTS D'ACCES A L'INTERNET.....	67
ANNEXES	69
ANNEXE 1 : COMPOSITION DU GROUPE DE TRAVAIL	69
ANNEXE 2 : AUDITIONS ET ENTRETIENS ENTREPRIS PAR LE GROUPE DE TRAVAIL.....	71
BIBLIOGRAPHIE.....	73

INTRODUCTION

L'internet, ce jeune média, est un nouvel espace de sociabilités. Il concerne aujourd'hui plus de 23 millions de Français et est particulièrement populaire auprès des jeunes. Comme d'autres médias, et comme d'autres espaces sociaux, il est susceptible d'être le lieu de la préparation et le théâtre de la représentation d'abus sexuels sur des mineurs.

Des opérations de police de grande ampleur sont régulièrement entreprises à l'encontre de personnes utilisant l'internet pour échanger des images pornographiques mettant en scène des mineurs. La presse se fait également l'écho de cas d'atteintes sexuelles commises sur des mineurs contactés par leurs agresseurs sur le réseau. En Grande-Bretagne, un rapport récent cite pédo-pornographie et pédophilie sur l'internet comme certaines des menaces de nature criminelle les plus préoccupantes sur l'internet¹.

Face à ce phénomène, certains Etats et instances internationales se sont déjà mobilisés : l'UNESCO a organisé une première réunion d'experts sur ces thèmes en 1999² ; et depuis plusieurs années, la lutte contre la diffusion d'images pédo-pornographiques sur l'internet figure à l'agenda des réunions du G8.

Cependant, pédo-pornographie et pédophilie sur l'internet continuent d'inquiéter. Le relatif anonymat – on pourrait parler de pseudonymat – qui a cours sur le réseau, ainsi que la facilité avec laquelle les techniques numériques permettent la reproduction et la diffusion à vaste échelle de tous types de contenus (textes, images, images animées...) alimentent ces craintes. Chacun connaît un enfant, un proche qui aurait été confronté à une situation ou un contenu préoccupant. Les rumeurs les plus diverses circulent et entretiennent auprès de certains un climat de méfiance face au réseau, perçu parfois comme le lieu de tous les dangers et de toutes les transgressions.

L'internet offre des libertés, des potentialités nouvelles à nos enfants. On ne peut plus revenir en arrière et imaginer un monde sans le réseau. Si celui-ci est porteur de nouveaux risques, parmi lesquels la pédo-pornographie ou la pédophilie comptent parmi les plus graves, nous devons les mesurer et organiser un plan de lutte. C'est l'objet du présent rapport.

Ce travail poursuit la réflexion du Forum des droits sur l'internet sur les usages des jeunes utilisateurs de l'internet. Il fait suite à un précédent rapport concernant "*l'exposition des mineurs à des contenus préjudiciables*³", remis en février 2004 aux ministres délégués à la Famille et à la Recherche et aux Nouvelles technologies.

Champ des recommandations

Pour bien comprendre les risques d'atteintes aux mineurs qui peuvent se réaliser sur l'internet, et que certains communément appellent "pédophilie sur internet", il convient de distinguer deux phénomènes :

- La diffusion et le recel de pornographie infantile (ou pédo-pornographie) sur l'internet ;
- L'utilisation du réseau internet aux fins de préparer ou de commettre des atteintes

¹ Sherridan MORRIS, *The future of netcrime now*, Home Office Online Report 62/04.

² Sexual Abuse of Children, Child Pornography and Paedophilia on the Internet: An international challenge - Expert Meeting, UNESCO, Paris, 18-19 January - http://www.unesco.org/webworld/child_screen/.

³ LE FORUM DES DROITS SUR L'INTERNET, *Les Enfants du Net - (1) Les mineurs et les contenus préjudiciables sur l'internet*, Le Forum des droits sur l'internet, 2004.

sexuelles sur des mineurs (corruption et tentative de corruption de mineurs, atteinte ou agression et tentative d'agression sexuelle, viol et tentative de viol, proxénétisme...).

Ces deux phénomènes sont distincts, mettent en cause des acteurs différents et appellent probablement des solutions de lutte spécifiques. Ils sont étudiés dans deux parties séparées.

L'analyse se concentre sur les contenus et les usages accessibles depuis les terminaux informatiques (micro-ordinateurs), qui constituent aujourd'hui de loin les points d'accès au réseau les plus communément employés. Cependant, l'accès et les usages de l'internet depuis les nouveaux terminaux, principalement les téléphones mobiles, dont les dernières générations proposent toutes sortes d'applications interactives, soulèvent des questions voisines ; celles-ci sont esquissées au sein de ce rapport et devront faire l'objet d'un travail ultérieur.

Enfin, il est clair que le rapport ne s'est pas cantonné à étudier ces phénomènes sur le *web*, mais prend en compte l'ensemble des protocoles de l'internet, les risques affectant les espaces interactifs (chats , forums...) ou les usages les plus nouveaux de l'internet (P2P ...) étant les plus mal connus.

Méthodologie

Les présentes analyses et recommandations résultent de la concertation, au sein du groupe de travail "Protection de l'enfance" du Forum des droits sur l'internet, de représentants des parties concernées par ce débat : représentants de l'administration (ministère de la Justice, Direction du développement des médias, Défenseur des enfants), des utilisateurs de l'internet et associations de protection des droits des enfants (Internet Society, Union nationale des associations familiales, Voix de l'Enfant) et des acteurs économiques (Association des fournisseurs d'accès et de services internet, MSN France, Orange France)⁴.

Le groupe de travail a procédé à l'audition de nombreux experts et acteurs concernés, au premier rang desquels des membres et responsables des forces de police et de gendarmerie⁵.

Ce rapport a fait l'objet d'une consultation des membres du Forum des droits sur l'internet du 21 décembre 2004 au 11 janvier 2005. Il a été définitivement adopté par le Conseil d'orientation du Forum le 21 janvier 2005, et rendu public le 25 janvier 2005.

⁴ La liste complète des membres du groupe de travail figure en annexe du présent rapport.

⁵ La liste complète des personnes entendues au cours de ces travaux figure en annexe du présent rapport.

I. LA DIFFUSION ET LE RECEL DE PEDO-PORNOGRAPHIE SUR L'INTERNET

En France, l'article 227-23 du Code pénal punit *"le fait [et sa tentative], en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique"*, ainsi que la diffusion, la détention, l'importation ou l'exportation de telles images ou représentations, quel qu'en soit le support de diffusion⁶.

La notion de pédo-pornographie peut poser certaines difficultés d'appréciation. En 2002, la Cour d'appel de Paris décrivait comme *"pornographiques"* les contenus d'un site internet figurant *"des organes génitaux féminins offerts, des organes génitaux masculins en érection et des actes de pénétration génitale, buccale, anale"*.⁷ En 1999, la Chambre criminelle de la Cour de cassation avait considéré que le caractère pornographique de documents *"mettant en scène des enfants ou adolescents, nus, jambes écartées, exhibant les organes sexuels, parfois en érection"*⁸ n'était pas contestable.

La décision-cadre du Conseil de l'Union européenne du 22 décembre 2003 relative à la lutte contre l'exploitation sexuelle des enfants et la pédo-pornographie définit la pédo-pornographie comme la représentation visuelle *"d'un enfant réel", "une personne réelle qui paraît être un enfant", ou "des images réalistes d'un enfant qui n'existe pas" "participant à un comportement sexuellement explicite ou s'y livrant, y compris l'exhibition lascive des parties génitales ou de la région pubienne"*.⁹

Pour l'Office international de police criminelle (Interpol), qui doit fédérer les définitions de la pédo-pornographie en vigueur auprès de ses différents membres, la pédo-pornographie peut être définie comme *"la description visuelle de l'exploitation sexuelle d'un enfant centrée sur le comportement sexuel de l'enfant ou sur ses parties génitales"*.¹⁰

Par ailleurs, certains contenus non strictement pornographiques, mais ouvertement érotiques ou faisant l'apologie de la pédophilie, qui n'entrent pas dans la qualification pénale française, devront être évoqués.

1. Evaluation générale du phénomène

a. Un phénomène d'importance observé sur la plupart des protocoles de l'internet.

Le premier constat qui s'impose en matière de diffusion et de recel de pédo-pornographie sur l'internet est que le volume, la typologie et la géographie des contenus sont mal connus. Des sources diverses, de fiabilité inégale, ne permettent pas de quantifier avec précision les faits et leur évolution dans une perspective française, mais indiquent des ordres de grandeur et des tendances : statistiques judiciaires, renseignements issus des signalements d'internautes auprès de services d'initiative publique ou privée, nationaux

⁶ Art. 227-23 du Code pénal.

⁷ CA Paris, 2 avril 2002, E.L. c/ Ministère Public.

⁸ C. cass. crim., 9 juin 1999, 98-80052.

⁹ Décision-cadre 2004/68/JAI du Conseil du 22 décembre 2003 relative à la lutte contre l'exploitation sexuelle des enfants et la pédopornographie. Journal Officiel n° L 13 du 20/01/2004. pp. 44-48. A noter qu'une décision-cadre lie les Etats membres quant au résultat à atteindre et laisse les instances nationales décider de la forme et des moyens pour ce faire, et ne s'inscrit pas dans le droit positif des Etats.

¹⁰ "Recommendations on Offences Against Minors", Interpol, 61e Assemblée générale (1995).

ou internationaux, statistiques établies à la suite de la recherche proactive de contenus, en France ou à l'étranger.

La perception diffuse d'un phénomène de réelle importance.

Régulièrement, des opérations de police d'une ampleur inédite sont engagées à l'encontre de diffuseurs et de receleurs d'images pédo-pornographiques sur l'internet, parfois à une échelle mondiale. En France, la première grande opération, intitulée "Forum 51", a été lancée par la gendarmerie nationale en juin 2001. Elle faisait suite à plus d'un an d'enquête sur certains canaux IRC (*Internet Relay Chat*), et a donné lieu à 75 interpellations en France. Lancée à l'initiative du *Federal Bureau of Investigation (FBI)* américain en 1998 dans 14 pays¹¹, l'opération "Cathédrale" aurait permis la découverte de 750 000 images pédo-pornographiques, l'identification de 1 263 victimes et l'appréhension de 108 suspects. En 2001, l'opération "Candyman" a mis au jour, à l'initiative du FBI américain, 3 groupes de discussion et d'échanges de fichiers basés sur le *web* et comptant 6 700 membres. Cette enquête a donné lieu à plus d'une centaine d'arrestations. Engagée dès 1999, et étendue à un niveau international en 2001, l'opération "Avalanche" a permis de faire cesser les opérations de la société *Landslide Productions*, basée à Fort Worth au Texas, qui diffusait sur plusieurs sites payants des images pédo-pornographiques importées, notamment, de Russie et d'Indonésie, et de saisir les coordonnées de 250 000 clients de cette société, localisés dans 37 Etats américains et 60 pays différents. Suite de l'opération "Avalanche" en Grande-Bretagne, l'opération "Ore" a conduit à l'interpellation, en janvier 2003, de 1 600 suspects sur le seul territoire britannique.

M. Yvon Tallec, chef du parquet des mineurs auprès du Tribunal de Grande Instance de Paris, constate "*une explosion*" récente et dans des proportions jusqu'alors inconnues du nombre de signalements de cas de détention, de recel et de diffusion de contenus pédo-pornographiques sur les supports informatiques. Le parquet parisien est parfois saisi plusieurs fois par jour de tels signalements¹². A elle seule, la Division nationale de la répression des atteintes aux biens et personnes (DNRAPB) de la Direction générale de la police judiciaire (DGPN), qui centralise la réception des signalements de diffusion ou de téléchargement de fichiers pédo-pornographiques sur l'internet en provenance de l'étranger, a reçu près de 3 000 de ces signalements au cours de l'année 2003. Elle mène de 40 à 50 interpellations par an sur la base de ces signalements, et défère autant de dossiers auprès du parquet de Nanterre¹³. Le groupe "technologies de l'information" de la Brigade de protections des mineurs (BPM) de la Direction régionale de la police judiciaire (DRPJ) de Paris a traité en 2003 96 affaires, majoritairement liées à des cas de diffusion et de recel de pornographie enfantine sur l'internet. Ce même groupe, dont les effectifs ont été renforcés, prévoyait de traiter près de 300 affaires l'année suivante, en 2004. Le chef d'escadron Eric Freyssinet, chef du département Informatique-Electronique (INL) de l'Institut de recherche criminelle de la gendarmerie nationale (IRCGN), prévoit également la hausse du nombre d'affaires, suite aux dernières affaires de masse instruites en France, et grâce à une coopération internationale de plus en plus active¹⁴.

La base centrale d'images pédo-pornographiques mise en place au sein de l'OIPC-Interpol recense 200 000 images saisies sur l'internet. Ce chiffre fournit un reflet atténué du nombre d'images en circulation permanente sur l'internet. Les enquêteurs auditionnés en préparation de ces travaux estiment que ce chiffre est en constante progression. Au 7

¹¹ Etats-Unis, Australie et pays d'Europe.

¹² Yvon TALLEC, audition du 8 juin 2004.

¹³ Marcel FAURE, audition du 27 avril 2004.

¹⁴ Eric FREYSSINET, entretiens des 14 et 18 octobre 2004.

septembre 2004, le Centre national d'analyse des images pédo-pornographiques (CNAIP) français avait recensé 471 501 photographies de nature pédo-pornographique¹⁵.

En "bout de chaîne", les statistiques issues du casier judiciaire ne décrivent que le nombre de condamnations prononcées pour une infraction particulière. Elles indiquent que 4 personnes ont été condamnées pour "*détention de l'image d'un mineur présentant un caractère pornographique*" en 2002, année de la création de l'infraction. Entre 2000 et 2002, 64, puis 22, puis 88 personnes ont été condamnées pour "*recel de bien provenant de la diffusion d'image d'un mineur à caractère pornographique*", sans que l'on puisse distinguer dans quelle mesure ces deux infractions sont liées à l'utilisation de l'internet. 3, 16 puis 10 personnes ont été condamnées sur le fondement de la "*diffusion de l'image d'un mineur présentant un caractère pornographique en utilisant un réseau de télécommunications*" (art. 227-23, al. 3 du Code pénal). Il est à noter que, considérant le délai moyen d'instruction des délits, ces chiffres fournissent très vraisemblablement un reflet des poursuites engagées dans les années 1998 à 2000.

Les indications issues des signalements et de la recherche de contenus pédo-pornographiques.

Le témoignage de Mme Catherine Chambon, chef de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) placé auprès du ministère de l'Intérieur, tend à confirmer le grand nombre de sources de pédo-pornographie sur l'internet et la relative faiblesse du nombre de cas connus de diffusion de tels contenus depuis la France ou par un ressortissant français. Au 15 avril 2004, après 29 mois d'existence, le point de signalement interministériel de contenus pédo-pornographiques, que gère l'OCLCTIC¹⁶, avait enregistré 14 000 signalements. Une moyenne stable de 10 à 12 % des contenus signalés avait paru de nature pédo-pornographique aux enquêteurs, après examen des contenus signalés. L'Office a transmis 800 signalements auprès d'autorités étrangères et réalisé 7 signalements à des parquets français la première année (2001). Aucun contenu hébergé en France n'a depuis été signalé à un parquet par l'Office¹⁷.

L'association de droit néerlandais InHope fédère les vingt points de signalement opérés, dans quatorze pays d'Europe, aux Etats-Unis, en Corée du Sud, en Australie et à Taiwan, par des acteurs associatifs et industriels. L'ensemble des points de signalement membres du réseau InHope ont recueilli entre mars 2003 et février 2004 96 217 signalements de contenus considérés par les déclarants comme pédo-pornographiques. Le Point de contact de l'Association française des fournisseurs d'accès et de services internet (AFA)¹⁸, membre fondateur d'InHope, est le correspondant du réseau en France. Le site Pointdecontact.net a reçu 1 777 signalements de contenus considérés comme pédo-pornographiques par les déclarants entre septembre 2002 et août 2003 inclus, et 1 390 signalements de ce type de septembre 2003 à août 2004 inclus. Entre mars et août 2004, 66,45% de l'ensemble des signalements de contenus tenus pour illicites par les "signalants" ont été considérés et traités comme tels par l'équipe en charge de la gestion du point de contact¹⁹. En Grande-Bretagne, la *hotline* de l'Internet Watch Foundation, membre elle aussi du réseau InHope, a reçu en 2003 plus de 15 000 signalements de contenus pédo-pornographiques²⁰.

¹⁵ Jacky DURAND, "Villepin pour une lutte Net et sans bavure", *Libération*, Paris, 8 septembre 2004.

Ce chiffre comprend les photographies et les images résultant du "découpage" de films pédo-pornographiques.

¹⁶ Voir : <http://www.internet-mineurs.gouv.fr/>

¹⁷ Catherine CHAMBON, audition du 27 avril 2004.

¹⁸ Voir : <http://www.pointdecontact.net/>

¹⁹ Sources Association des Fournisseurs d'Accès et de Services Internet (AFA).

²⁰ INTERNET WATCH FOUNDATION, *Annual Report 2003*, London, 2003.

Aux Etats-Unis, la *CyberTipline* du *National Center for Missing and Exploited Children* (NCMEC) a vu le nombre des signalements de contenus pédo-pornographiques qui lui sont adressés évoluer de 1 393 en 1998 à 26 759 en 2002²¹. Il convient toutefois de noter que, lus en tendance, les chiffres rapportés par les points de contact renvoient une image de l'évolution de la diffusion de contenus pédo-pornographiques sur l'internet largement déformée par l'évolution de la visibilité de ces points de contact et du "réflexe" consistant à leur signaler les contenus illicites.

Depuis 1996, les membres de l'association Le Bouclier identifient les documents pédo-pornographiques et leurs diffuseurs sur l'internet, tout particulièrement sur le *web*. Une étude portant sur les années 1996 à 2002 synthétise le produit des recherches de l'association. D'après ce document, Le Bouclier aurait dénombré 261 653 "sites pédophiles" en 2002, contre 4 300 seulement en 1996. Les sites commerciaux devanceraient les sites de particuliers et "militants". Certaines imprécisions de nature méthodologique concernant, notamment, la nature exacte de ces sites (pédo-pornographie, images tendancieuses représentant des enfants dénudés, apologies de la pédophilie) doivent toutefois faire considérer ces chiffres alarmants avec circonspection²².

Arcobaleno Telefono, une autre association basée en Italie, procède également à la recherche active de contenus pédo-pornographiques sur le *web*. Elle déclare avoir identifié et signalé aux autorités 17 016 sites à caractère "pédophile et pédo-pornographique" en 2003, un chiffre en très forte augmentation comparé à celui de 2002. Ces chiffres, qui ne sont certifiés par aucune autorité et dont la pertinence ne peut être garantie, sont encore cités à titre indicatif.

Applications et protocoles exploités au profit de la diffusion de pédo-pornographie.

La plupart des signalements adressés aux points de contact portent sur des contenus rencontrés sur le *web*. Les contenus pédo-pornographiques accessibles depuis cette "vitrine" de l'internet ne représentent toutefois que la partie la plus visible d'un ensemble plus vaste d'images échangées.

Entre 1998 et 2003, le point de signalement américain du NCMEC²³ a reçu 76 000 signalements, dont 77 % concernaient le *web*, et 1% seulement les réseaux P2P. Ce dernier chiffre paraît toutefois en rapide évolution au fur et à mesure que les usages des réseaux P2P gagnent en popularité : en 2001, 156 des signalements de contenus pédo-pornographiques adressés au NCMEC concernaient les réseaux P2P. En 2002, 757 de ces signalements s'y rapportaient. Les statistiques du NCMEC indiquent également une augmentation régulière des signalements se rapportant au *web* (de 18 052 à 26 759 entre 2001 et 2002) et, surtout, au courrier électronique (de 1 128 à 6 245 entre 2001 et 2002), sous la pression, sans doute, de l'augmentation du nombre de messages publicitaires pornographiques non sollicités diffusés via le réseau. On remarque enfin d'après ces indicateurs que le nombre de signalements se rapportant aux autres protocoles (*newsgroups* - groupes de discussion, *chat rooms* - salons de discussion, messagerie instantanée, FTP - transferts de fichiers) évoluent dans de moindres proportions²⁴.

²¹ Voir Figure 1.

²² LE BOUCLIER, "Pédocriminels impunis. Extrait partiel des résultats de l'étude des sites Internet pédophiles menée par l'association Le Bouclier de 1996 à 2002 portant sur 261.653 sites", 2003.

²³ Voir : <http://www.cybertipline.com/>

²⁴ Cité par UNITED STATES GENERAL ACCOUNTING OFFICE, *File-Sharing Programs. Peer-to-Peer Networks Provide Ready Access to Child Pornography*, Ibid, p. 8.

Technology	Number of tips				
	1998	1999	2000	2001	2002
Web sites	1,393	3,830	10,629	18,052	26,759
E-mail	117	165	120	1,128	6,245
Peer-to-peer	—	—	—	156	757
Usenet newsgroups & bulletin boards	531	987	731	990	993
Unknown	90	258	260	430	612
Chat rooms	155	256	176	125	234
Instant Messaging	27	47	50	80	53
File Transfer Protocol	25	26	58	64	23
Total	2,338	5,569	12,024	21,025	35,676

Source: Exploited Child Unit, National Center for Missing and Exploited Children.

Figure 1. Signalements transmis par le NCMEC aux organismes gouvernementaux chargés de réprimer la diffusion de pornographie enfantine (FBI, Division criminelle du Département de la Justice, Douanes).

En 2003, les signalements adressés à l'*Internet Watch Foundation*, concernaient en très grande majorité des contenus accessibles sur le *web*, et plus rarement sur les groupes de discussion (*Usenet*) et certains services communautaires²⁵.

Une étude de février 2003 du *General Accounting Office* (GAO) américain établit que les réseaux *peer-to-peer* (P2P) constituent un canal de plus en plus souvent utilisé pour l'échange d'images pédo-pornographiques²⁶ : sur 341 images téléchargées et examinées par les douanes américaines à la suite de requêtes portant sur trois mots clés fréquemment associés aux contenus pédo-pornographiques, 149 images (soit 44% environ) se sont avérées être de nature pédo-pornographique. Ces éléments permettent au GAO de conclure que les applications d'échange de fichiers de pair à pair permettent un accès aisé à ces contenus.

Le nombre de sites *web* pédo-pornographiques hébergés en France est faible. Aussi les enquêtes de l'IRCGN, par exemple, s'orientent plus souvent, selon le chef de son département informatique²⁷, vers les réseaux P2P et sur les différents espaces publics de l'internet : forums sur Usenet (*newsgroups*), *Internet Relay Chat* (IRC), *chats* sur le *web*, forums sur le *web*, *chats* proposés par certains fournisseurs de services internet...

Selon M. Philippe Jarlov, gendarme spécialisé de la section des recherches de Bordeaux, le réseau UnderNet, l'un des réseaux IRC les plus étendus, compterait ainsi de 15 à 20 salons de discussion consacrés aux échanges d'images pédo-pornographiques ou de propos "pédophiles". Ce gendarme déclare identifier chaque année, sur le protocole IRC, 10 à 20 diffuseurs de fichiers pédo-pornographiques localisés en France, et chaque semaine de 10 à 15 utilisateurs de réseaux P2P localisés en France et offrant des images pédo-pornographiques au téléchargement²⁸. Il convient de noter qu'une part non négligeable de ces diffuseurs ont pu se faire les relais involontaires de ces contenus : en téléchargeant en masse des groupes de fichiers sur les réseaux IRC ou P2P, certains

²⁵ INTERNET WATCH FOUNDATION, op. cit.

²⁶ UNITED STATES GENERAL ACCOUNTING OFFICE, *File-Sharing Programs. Peer-to-Peer Networks Provide Ready Access to Child Pornography, Report to the Chairman and Ranking Minority Member*. GAO-03-351, Committee on Government Reform, House of Representatives, Washington, DC, February 2003.

²⁷ Eric FREYSSINET, entretiens des 14 et 18 octobre 2004.

²⁸ Philippe JARLOV, audition du 14 septembre 2004.

utilisateurs sont susceptibles d'enregistrer et de redistribuer aussitôt certains contenus illicites, sans même avoir pris connaissance de la nature de ces contenus.

On peut conclure de cet ensemble de sources et de commentaires que la pédopornographie est bien présente sur l'internet, le nombre de sources et de personnes impliquées se chiffrant en dizaine de milliers dans le monde. Certaines applications (IRC, P2P) semblent avoir la préférence des diffuseurs et receleurs de matériels pédopornographiques, mais tous les protocoles de l'internet et ses espaces publics sont mis à profit par ces derniers, sans toutefois que ces contenus y soient systématiquement visibles. Si les éléments manquent pour affirmer avec certitude que l'internet est le vecteur d'un commerce accru de pédopornographie, il est peu contestable que ces contenus y sont plus accessibles que par les médias traditionnels. Ces observations, toutefois, ne permettent pas de saisir quelle économie sous-tend l'échange de ces contenus illicites, ni d'ailleurs la part des contenus accessibles gratuitement face à celle des services payants. Il est en revanche certain que, comme dans la plupart des modèles connus de circulation de biens immatériels, l'échange gratuit de fichiers entre "collectionneurs" coexiste avec des services rémunérés. La fréquence du recours à la cryptologie aux fins de dissimuler les fichiers pédopornographiques échangés, enfin, reste impossible à estimer, même si plusieurs enquêtes ont confirmé l'usage de cet ensemble de techniques au sein de certains réseaux d'échange d'images pédopornographiques.

b. Les serveurs d'images pédopornographiques sur le web concentrés géographiquement.

Les statistiques officielles décrivent mal la progression de la diffusion et du recel d'images pédopornographiques sur l'internet, et ne donnent qu'un aperçu flou de l'origine de ces contenus. Il convient à nouveau, pour s'en faire une idée, de croiser des informations issues de plusieurs sources.

Les signalements de contenus pédopornographiques transmis aux *hotlines* désignent le plus souvent des images accessibles sur le *web*. Ces dernières représentent la "partie émergée" et souvent marchande de l'échange et du recel de pédopornographie sur l'internet.

D'après Mme Chambon, chef de l'OCLCTIC, ces contenus sont schématiquement localisés pour un tiers aux Etats-Unis, pour un tiers en Fédération de Russie, et pour un dernier tiers dans une variété d'autres pays²⁹.

Le rapport annuel de l'Internet Watch Foundation confirme ce constat : 55% des contenus pédopornographiques qui ont été signalés à la *hotline* britannique étaient hébergés aux Etats-Unis, 23% en Russie, 6% en Europe, 4% au Brésil et 4% en Corée du Sud.

Enfin, l'association italienne *Telefono Arcobaleno* situe les 17 016 sites "pédophiles et pédopornographiques" qu'elle a signalés aux autorités dans 33 pays, et en premier lieu aux Etats-Unis (61,72%), en Corée du Sud (7,95%), en Russie (7,24%) et au Brésil (7,24%). 43 serveurs (soit 0,25% de son activité) localisés en France ont été signalés par l'association.

Les sites pédopornographiques sont souvent décrits comme extrêmement "mobiles" et susceptibles, lorsqu'ils sont identifiés par les services de police et de gendarmerie, de changer très rapidement de serveur d'hébergement et d'adresse.

²⁹ Catherine CHAMBON, audition du 27 avril 2004.

Ces éléments d'appréciation, qui concernent pour l'essentiel les contenus pédo-pornographiques accessibles sur le *web*, ne donnent à nouveau qu'une image imprécise de la localisation de l'ensemble des serveurs de fichiers pédo-pornographiques. En particulier, ils ne rendent pas compte de l'échange de matériels pédo-pornographiques entre individus *via* d'autres applications de l'internet, qui constitue sans doute une part importante des infractions commises en France.

c. Faut-il craindre que l'internet banalise la pédo-pornographie ?

Un rapport consacré en 2003 par la Direction générale des droits de l'homme du Conseil de l'Europe sur *"l'impact de l'utilisation des nouvelles technologies de l'information sur la traite des êtres humains aux fins d'exploitation sexuelle"* rapporte qu'aux Etats-Unis, le nombre d'affaires liées à l'utilisation de l'internet traitées par l'*US Postal Service* auraient régulièrement crû, passant de 32% en 1998 à 47% en 1999 et 77% en 2000. Toutefois, l'*US Postal Inspection Service* "a [également] pu constater que l'utilisation accrue de l'Internet par les pédo-criminels s'est traduite parallèlement par une progression de leur recours aux services postaux³⁰." Ce constat suggère que, après avoir connu un pic dans les années 1970, puis reculé sous la pression de la généralisation de la régulation de ces contenus en Europe et aux Etats-Unis entre les années 1970 et 1990³¹, la distribution de pédo-pornographie pourrait connaître un regain à l'âge des médias électroniques.

Les interprétations des chiffres de la diffusion de pornographie infantine sur l'internet divergent toutefois. A l'idée que l'internet rend possible la massification et la banalisation de l'échange d'images pédo-pornographiques à l'échelle planétaire, répond la thèse selon laquelle la diffusion d'images pédo-pornographiques sur l'internet ne fait que rendre plus visible un phénomène largement préexistant au réseau et à ses applications.

La réalité participe sans doute des deux lectures du phénomène, et il convient de porter ici quelques observations :

- La perception de la diffusion de pédo-pornographie sur l'internet et le nombre d'affaires judiciaires liées à ce phénomène vont croissants ;
- La diffusion d'images pédo-pornographiques sur l'internet reste toutefois sans commune mesure avec celle de pornographie adulte, qui s'est constituée en l'un des secteurs d'activité les plus florissants du réseau³² ;
- Certaines images pédo-pornographiques ne circulant plus seulement sous plis scellés, mais étant librement accessibles sur le réseau sous une apparence d'anonymat renforcée, il paraît probable que certaines personnes qui n'auraient pas fait la démarche de rechercher puis d'acquérir des contenus pédo-pornographiques auprès de revendeurs "traditionnels" ont pu y accéder, souvent gratuitement, sur l'internet³³ ;
- La terminologie propre à la pédo-pornographie paraît avoir largement "contaminé" sur l'internet la pornographie adulte : les sites diffusant de la

³⁰ *L'impact de l'utilisation des nouvelles technologies de l'information sur la traite des êtres humains aux fins d'exploitation sexuelle. Rapport final du groupe de spécialistes EG-S-NT.* Conseil de l'Europe, Direction générale des droits de l'homme, Division égalité entre les femmes et les hommes. Strasbourg, Septembre 2003. pp.14-15.

³¹ Margaret A HEALY, *Child pornography: an international perspective*, Computer Crime Research Center, août 1996.

³² Voir LE FORUM DES DROITS SUR L'INTERNET, op. cit.

³³ Voir Roger DARLINGTON, "Sex on the Net", 2 août 2004.

pornographie adulte prétendant diffuser des images de "preteens" ("pré-adolescentes") sont aujourd'hui innombrables, banalisant les codes de la pédo-pornographie, sinon ses représentations.

On ne peut guère établir, au vu des éléments recueillis, que la diffusion d'images pédo-pornographiques sur l'internet concoure à la "banalisation" de tels contenus. Seule la veille systématique de l'exploitation de l'internet aux fins de diffusion de pédo-pornographie pourrait indiquer si l'internet a créé, en facilitant l'accès à ces contenus, les conditions d'un renouvellement du marché de la pédo-pornographie.

2. Etat des moyens en vue de combattre la diffusion et le recel de pornographie enfantine sur l'internet, et des limites de ces moyens

a. Analyse des dispositifs pénaux réprimant le recel et la diffusion de pornographie enfantine.

En engageant les Etats signataires à prendre les dispositions appropriées pour empêcher que "*des enfants ne soient exploités aux fins de la production de spectacles ou de matériel de caractère pornographique*", la Convention internationale relative aux Droits de l'Enfant du 20 novembre 1989 (art. 34) identifie la pédo-pornographie comme une violation des droits des enfants. Les dispositions en condamnant la production, la diffusion et la détention restent pourtant diversement intégrées dans les droits internes.

En France, un dispositif pénal complet.

L'article 227-23 du Code pénal punit de 45 000 euros d'amende et de trois ans de prison le fait de fixer, d'enregistrer, de transmettre, de diffuser, d'importer ou d'exporter l'image ou la représentation à caractère pornographique d'un mineur de moins de 18 ans ou d'une personne dont l'aspect physique est celui d'un mineur, sauf s'il est établi que cette personne était âgée de 18 ans au jour de la fixation ou de l'enregistrement de son image. Depuis la loi pour la confiance dans l'économie numérique du 21 juin 2004 est punie de la même peine la tentative de fixation, d'enregistrement ou de transmission d'une telle image ou représentation en vue de sa diffusion. Les peines sont portées à cinq ans d'emprisonnement et à 75 000 euros d'amende lorsqu'un réseau de télécommunications (ou communications électroniques) a été utilisé pour diffuser l'image ou la représentation du mineur à destination d'un public non déterminé. Depuis la loi du 4 mars 2002 relative à l'autorité parentale, enfin, le fait de détenir une telle image ou représentation est puni de deux ans d'emprisonnement et 30 000 euros d'amende.

Une spécificité de l'article 227-23 doit être soulignée : il protège les mineurs victimes, mais également, depuis la loi du 17 juin 1998, l'*image* des mineurs, en punissant la représentation pornographique d'un mineur, même virtuelle (montage, dessin...)³⁴, ce qui fait du Code pénal français un dispositif particulièrement protecteur.

Le recel d'images pédo-pornographiques, soit "*le fait de dissimuler, de détenir ou de transmettre une chose, ou de faire office d'intermédiaire afin de la transmettre, en sachant que cette chose provient d'un crime ou d'un délit*" et "*le fait, en connaissance de cause, de bénéficier, par tout moyen, du produit d'un crime ou d'un délit*", est puni de

³⁴ Loi n°98-468 du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des enfants, art. 17.

cinq ans et de 375 000 euros *d'amende* (art. 321-1 et suivants du Code pénal)³⁵. Cette incrimination a souvent servi, avant l'adoption de la loi du 4 mars 2002, à punir la simple détention d'images pédo-pornographiques.

De l'avis de M. Yvon Tallec, chef du parquet des mineurs du TGI de Paris, l'article 227-23 pose, en pratique, des difficultés d'appréciation du caractère pornographique des images. En effet, de nombreuses images en circulation sur le réseau sont d'une nature ambiguë. Elles présentent par exemple parfois les protagonistes majeurs de scènes pornographiques comme mineurs, ou représentent des personnes mineures dans des scènes de nu aux limites de la pornographie. Des enquêteurs notent que l'appréciation de la nature "pornographique" d'une représentation ou de la minorité d'âge présumée d'une personne varie selon les juridictions. La minorité des personnes représentées ne peut toutefois être mise en doute dans la plupart des affaires dont se saisissent les services d'enquête³⁶.

Des enquêteurs de la brigade parisienne de protection des mineurs (BPM) notent qu'en moyenne, la détention d'images est punie dans leur juridiction de peines de 2 à 3 mois de prison avec sursis, et la diffusion de ces contenus d'une peine de 6 à 8 mois de prison avec sursis, souvent assortie d'un contrôle socio-judiciaire³⁷. Ces indications sont à rapprocher des statistiques du casier judiciaire, qui indiquent que l'infraction de recel de biens provenant de la diffusion de l'image d'un mineur à caractère pornographique a été punie en moyenne, entre 2000 et 2002, de peines d'emprisonnement avec sursis dans près de 9 condamnation prononcée sur 10 et, plus rarement, de 5,5 à 14 mois d'emprisonnement ferme. Les informations disponibles ne permettent toutefois pas de savoir combien de ces condamnations sont liées à l'utilisation de l'internet, ni si les contrevenants ont retiré un profit du recel de ces images.

Année	2000	2001	2002	Moyenne
Condamnations (condamnations portant sur cette infraction à titre principal)	64	22	88	58,00
Emprisonnement	64	20	83	55,67
Soit, en pourcentage des condamnations prononcées	100,00%	90,91%	94,32%	95,08%
... dont emprisonnement ferme	2	2	23	9,00
Soit, en pourcentage des condamnations prononcées	3,13%	9,09%	26,14%	12,78%
Quantum ferme de l'emprisonnement ferme (mois)	7,5	5,5	14,8	9,27
Amendes	0	1	4	1,67
Soit, en pourcentage des condamnations prononcées	0,00%	4,55%	4,55%	3,03%
Montant moyen de l'amende ferme	0,00 €	1 219,60 €	1 000,00 €	1 109,80 €

Figure 2. Recel de bien provenant de la diffusion d'image d'un mineur à caractère pornographique. Source : Casier judiciaire.

Le nombre de condamnations pour détention de l'image d'un mineur présentant un caractère pornographique est encore faible en 2002, année de création de l'infraction, en comparaison du nombre de condamnations pour recel, mais enregistre une nette augmentation en 2003. L'évolution de cette tendance reste à confirmer.

³⁵ Un exemple de décision rendu sur le fondement du recel d'images pédo-pornographiques : Tribunal de grande instance du Mans, jugement correctionnel, 16 février 1998, Monsieur le Procureur de la République c/ Ph. H.

³⁶ Yvon TALLEC, audition du 8 juin 2004.

³⁷ Marie LAJUS, Fabrice GAUTHIER, audition du 11 mai 2004.

Année	2002	2003
Condamnations (ensemble des condamnations portant cette infraction, à titre principal ou secondaire)	6	39
Emprisonnement (condamnations portant cette infraction à titre principal exclusivement)	2	9
... dont emprisonnement ferme	1	1
Quantum ferme de l'emprisonnement ferme (mois)	2	2
Amendes	3	3
Montant moyen de l'amende ferme	1 000,00 €	1 167 €

Figure 3. Détention de l'image d'un mineur présentant un caractère pornographique. Source : Casier judiciaire.

Les condamnations prononcées à l'encontre des auteurs de faits de diffusion d'images pédo-pornographiques *"en utilisant un réseau de télécommunication"* sont également majoritairement punies de peines d'emprisonnement avec sursis et, plus rarement, de 3 à 8 mois d'emprisonnement ferme.

Année	2000	2001	2002	2003	Moyenne
Condamnations (ensemble des condamnations portant cette infraction, à titre principal ou secondaire)	7	21	24	52	26
Emprisonnement (condamnations portant cette infraction à titre principal exclusivement)	0	10	7	19	12
... dont emprisonnement ferme	-	1	1	7	2,25
Quantum ferme de l'emprisonnement ferme (mois)	-	4	8	6,4	4,6
Amendes	-	1	1	-	0,5
Montant moyen de l'amende ferme	-	3000 F	750€		603 €

Figure 4. Diffusion de l'image d'un mineur présentant un caractère pornographique en utilisant un réseau de télécommunications. Source : Casier judiciaire.

Le nombre de condamnations prononcées, relativement faible, doit être considéré en tenant compte du fait que les procédures entreprises en masse à la suite de récentes enquêtes d'envergure nationale et internationale sont aujourd'hui encore en cours d'instruction : la durée moyenne de l'instruction des délits s'élevait en 2002 à 17,7 mois³⁸.

Si le code pénal réprime sévèrement la détention, la diffusion, l'enregistrement, la fixation et la production de représentation à caractère pornographique, il n'incrimine pas les incitations à commettre des viols ou agressions sexuelles qui ne seraient pas suivies d'effets. Un amendement sénatorial visant directement la diffusion de tels messages sur l'internet, avait ainsi été rejeté au cours de la discussion du projet de loi relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des enfants au motif, selon les mots du rapporteur du texte, qu' *"aux termes de l'article 23 de la loi de 1881 sur la presse, sont considérés comme complices ceux qui incitent directement à commettre un crime ou un délit, à condition que la provocation ait été suivie des faits, voire d'une tentative de crime"*³⁹. On note que cette provocation est notamment punissable lorsqu'elle est commise par *"tout moyen de communication au public par voie*

³⁸ Ministère de la Justice, "Les chiffres clés de la justice - Justice pénale" - <http://www.justice.gouv.fr/chiffres/penale03.htm>.

³⁹ Charles JOLIBOIS, Rapporteur du projet de loi devant le Sénat, Sénat, Séance du 30 octobre 1997 - http://www.senat.fr/seances/s199710/s19971030/s19971030_mono.html.

électronique", en vertu de l'article 2 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique.

Unanimité et nuances des législations pénales européennes.

L'ensemble des pays d'Europe met en œuvre une législation permettant de lutter contre la pédo-pornographie, c'est-à-dire d'empêcher la production, la diffusion, et même, souvent, la détention de telles représentations. Ces infractions sont diversement sanctionnées. Certaines de ces dispositions, comme celles punissant la détention de pornographie enfantine, sont d'adoption récente, même dans les pays réprimant de longue date la production et la diffusion de tels matériels comme la France⁴⁰.

L'Union européenne s'est également saisie de ces questions. Le Conseil a adopté le 24 février 1997 une *"action commune relative à la lutte contre la traite des êtres humains et l'exploitation sexuelle des enfants"*. Par elle, les Etats membres acceptaient d'ériger en infractions pénales certains comportements comme *"l'exploitation sexuelle des enfants aux fins de la production (...) de matériel à caractère pornographique, y compris la production, la vente et la distribution ou d'autres formes de trafic de matériel de ce type, et la détention de ce type de matériel"*⁴¹.

La décision du Conseil du 29 mai 2000 *"relative à la lutte contre la pédopornographie sur Internet"*⁴² a renforcé les mesures de prévention et de lutte contre la production, la diffusion et la détention d'images pédo-pornographiques. Elle a fixé des objectifs de répression effective de ces comportements, de coopération des points de contact spécialisés assurant une veille permanente du phénomène, et de coopération des acteurs étatiques et industriels au niveau national dans le *"but d'empêcher et de combattre l'exploitation sexuelle des enfants et, en particulier, la production, le traitement, la diffusion et la détention de matériel pédopornographique sur internet."*

Ces principes constituent les principales orientations du Plan d'action pour un internet plus sûr (*Safer Internet Action Plan*) de la Commission européenne. Ce plan d'action pluriannuel comporte par exemple, depuis sa mise en place en 1998, une ligne d'action tendant à *"créer un réseau européen de lignes directes"* de signalement des contenus illicites. 5,88 millions d'euros étaient consacrés par le programme de travail 1999-2002 au développement de ces lignes directes ; 3,3 millions d'euros y ont été alloués dans le programme de travail 2002-2004⁴³. De 2005 à 2008, la Commission européenne investira encore 45 millions d'euros dans ce plan d'action⁴⁴.

Abrogeant l'action commune de 1997, la décision-cadre 2004/68/JAI du Conseil du 22 décembre 2003 relative à la lutte contre l'exploitation sexuelle des enfants et la pédo-pornographie, unifie les législations pénales des Etats membres. Elle prend spécifiquement en compte les risques liés à la diffusion de tels matériels sur les réseaux en précisant que *"la pédopornographie (...) prend de l'ampleur et se propage par le biais*

⁴⁰ "La lutte contre la pornographie enfantine". *Les documents de travail du Sénat. Série Législation comparée.* N°LC 90. Sénat. Service des Affaires européennes. Paris. 18 mai 2001.

⁴¹ Action commune 97/154/JAI du 24 février 1997 adoptée par le Conseil relative à la lutte contre la traite des êtres humains et l'exploitation sexuelle des enfants.

⁴² Décision 2000/375/JAI du Conseil du 29 mai 2000 relative à la lutte contre la pédopornographie sur l'internet. Journal Officiel n° L 138 du 09/06/2000. pp. 1-4.

⁴³ Les programmes de travail du Plan d'Action pour un Internet plus sûr (*Internet Action Plan*) peuvent être consultés à l'adresse : http://europa.eu.int/information_society/programmes/iap/programmes/workprogramme/text_en.htm.

⁴⁴ Voir : http://europa.eu.int/information_society/activities/sip/news_events/saferinternet_plus/index_en.htm. La proposition de décision instituant le plan *"Safer Internet Plus"* a été agréée par le Conseil le 2 décembre 2004.

de l'utilisation des nouvelles technologies et de l'internet⁴⁵." La décision-cadre définit la pédo-pornographie comme la représentation visuelle "d'un enfant réel", "une personne réelle qui paraît être un enfant", ou "des images réalistes d'un enfant qui n'existe pas" "participant à un comportement sexuellement explicite ou s'y livrant, y compris l'exhibition lascive des parties génitales ou de la région pubienne". Alors que les législations nationales fixaient l'âge à partir duquel peut être faite la représentation pornographique d'une personne entre 14 et 18 ans, le texte impose l'âge de 18 ans, sans toutefois modifier l'âge de la majorité sexuelle dans les Etats membres. La décision-cadre a enfin pour objet d'uniformiser les législations européennes en requérant que des peines privatives de liberté maximales de un à trois ans soient prévues à l'encontre des personnes qui produisent, distribuent, diffusent, transmettent, acquièrent et détiennent du matériel pédo-pornographique.

Une illustration de l'hétérogénéité des dispositifs pénaux dans le monde.

Etats-Unis.

Souvent dénoncés comme le territoire hébergeant le plus grand nombre de serveurs d'images pédo-pornographiques, les Etats-Unis disposent pourtant d'un dispositif pénal complet en matière de lutte contre la production, la diffusion et la détention de ce type de contenus, qui a inspiré pour partie la décision-cadre européenne.

Une succession de textes adoptés depuis 1977 ont défini un cadre prohibant la détention, la production et la diffusion de représentations pornographiques de mineurs de moins de 18 ans. L'article 2251 du Code fédéral condamne ainsi la production d'images d'un enfant de moins de 18 ans "se livrant à un comportement sexuellement explicite", ce dernier étant défini comme les relations sexuelles, quelle que soit leur nature, la zoophilie, la masturbation, les violences sado-masochistes et l'exhibition lascive des parties génitales ou de la région pubienne. L'article 2252 du Code fédéral punit la diffusion et la possession d'images représentant une telle scène réalisée ou simulée avec la participation effective d'un mineur. Le Code fédéral ajoute une circonstance aggravante à l'infraction lorsque les images possédées ou diffusées ont franchi une frontière.

Le *Child Pornography Prevention Act* (CPPA), qui avait pour objectif de criminaliser les représentations pédo-pornographiques virtuelles, rendues possibles par les nouvelles techniques de traitement de l'image, a été jugé inconstitutionnel par la Cour suprême le 16 avril 2002 en vertu des dispositions du Premier amendement à la Constitution, la prohibition de la représentation d'images d'enfants fictifs paraissant susceptible d'entraver la création artistique⁴⁶.

En conclusion, ce n'est pas dans d'éventuelles carences de la législation qu'il convient de rechercher les causes de la récurrence des signalements de serveurs d'images pédo-pornographiques hébergés sur le territoire des Etats-Unis. D'autres explications peuvent être avancées, comme par exemple le grand nombre de services d'hébergement de sites *web* gratuits ou à bas prix situés sur le territoire des Etats-Unis⁴⁷, ou le fait que les

⁴⁵ Décision-cadre 2004/68/JAI du Conseil du 22 décembre 2003 relative à la lutte contre l'exploitation sexuelle des enfants et la pédopornoigraphie. Journal Officiel n° L 13 du 20/01/2004. pp. 44-48.

⁴⁶ Agathe Lepage, *Libertés et droits fondamentaux à l'épreuve de l'internet*, Editions du Juris-Classeur, Paris, 2002, pp. 176-177

⁴⁷ Pour l'association Le Bouclier, "Plus de la moitié des sites pédophiles sont hébergés sur des machines se situant physiquement sur le territoire des Etats-Unis et du Canada. Les sites « russes » sont pour la plupart installés sur des serveurs américains et font partie de ceux qui produisent le plus de richesses en offrant à la vente des vidéos (...)". Le Bouclier, op. cit.

autorités américaines semblent plutôt concentrer une grande partie de leurs efforts sur la lutte contre les contact entre de potentiels agresseurs sexuels et des enfants sur l'internet.

Japon.

Longtemps désigné comme une source importante de pornographie enfantine, le Japon a mis en place, en 1999, une législation pénale adaptée. La loi *"punissant les actes liés à la prostitution enfantine et à la pédo-pornographie"* rend illégales la production, la diffusion et la vente de pédo-pornographie. La diffusion de pornographie enfantine sur l'internet peut ainsi être punie de trois ans d'emprisonnement.

Fédération de Russie.

La Fédération de Russie est fréquemment désignée, au côté des Etats-Unis, comme l'un des pays hébergeant le plus grand nombre de serveurs pédo-pornographiques, et comme un territoire où la production de tels contenus reste active.

Le Code pénal russe punit la production non autorisée de contenus pornographiques à des fins de diffusion, quelque soit le support, mais ne prévoit pas de dispositions particulières en matière de pédo-pornographie, ni ne réprime spécifiquement la diffusion, l'acquisition ou la détention de pornographie. La production de contenus pédo-pornographiques est toutefois susceptible d'être poursuivie comme une infraction sexuelle commise sur un mineur.

Malgré le "non alignement" de son droit pénal, la Russie participe au groupe de lutte contre la pédo-pornographie qui se réunit au sein du G8, et a pris part à quelques initiatives ponctuelles en matière de coopération judiciaire, comme l'opération "Blue Orchid", qui a abouti en 2001 au démantèlement d'un réseau de production de pédo-pornographie par les douanes américaines et la police de Moscou.

Les apports de la Convention sur la cybercriminalité.

La Convention sur la cybercriminalité du Conseil de l'Europe, adoptée à Budapest par le Comité des ministres le 8 novembre 2001, est le premier traité international portant en particulier sur les infractions liées à la criminalité informatique et, notamment, à la pornographie enfantine sur l'internet. Son principal objectif, énoncé dans le préambule, est de poursuivre *"une politique pénale commune destinée à protéger la société contre le cybercrime, notamment par l'adoption d'une législation appropriée et la stimulation de la coopération internationale"*⁴⁸.

L'article 9 de la Convention fait ainsi de la production de pornographie enfantine en vue de sa diffusion par le biais d'un système informatique, de l'offre ou de la mise à disposition, du fait de se procurer ou de procurer à autrui, ou encore de la possession de pornographie enfantine dans ou par un système informatique, une infraction destinée à être traduite dans le droit interne de l'ensemble des pays signataires. "Pornographie enfantine" est ici entendu comme la représentation visuelle d'*"un mineur se livrant à un comportement sexuellement explicite"*, d'*"une personne qui apparaît comme un mineur*

⁴⁸ Conseil de l'Europe, Convention STE n°185 sur la Cybercriminalité, 8 novembre 2001.

se livrant à un comportement sexuellement explicite", ou "des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite." Le terme "mineur" désigne dans la Convention toute personne âgée de moins de 18 ans ; un Etat-partie peut toutefois fixer une limite d'âge inférieure, qui doit être au minimum de 16 ans.

Signé au 30 septembre 2004 par trente-huit des quarante-cinq Etats représentés au Conseil de l'Europe, dont les Etats-Unis, et ratifié par huit d'entre eux seulement, au nombre desquels ne figure pas la France⁴⁹, le traité est entré en vigueur le 1er juillet 2004. La Russie n'a pas signé ce traité.

Il ressort de cette brève analyse de quelques-uns des régimes applicables à la diffusion de pédo-pornographie sur l'internet que les carences en matière pénale ne peuvent expliquer à elles seules la persistance et l'accroissement de la diffusion de pédo-pornographie sur l'internet.

b. Organisation et moyens des services d'enquête en France.

La poursuite des actes de production, de diffusion et de détention d'images pédo-pornographiques liés à l'internet fait intervenir, en France, différents services de police et de gendarmerie, spécialisés ou non.

Services de police.

La Division nationale de répression des atteintes aux biens et personnes (DNRAPB) anime depuis 1997 un groupe de six enquêteurs formés et dédiés aux enquêtes sur l'internet. Ce service observe une croissance exponentielle des signalements qui lui sont adressés, qui sont passés de 300 à 400 signalements au cours des dernières années à plus de 3 000 signalements en 2004, tandis que le nombre de personnels que la division consacre à ces affaires est demeuré inchangé. La DNRAPB traite en propre près de 10% des affaires qui lui sont signalées, et transmet le solde aux juridictions dont relèvent les suspects identifiés. La plupart des signalements transmis à la DNRAPB font suite à la saisie d'adresses IP et de coordonnées de cartes bancaires françaises par des autorités étrangères, qui les transmettent en masse aux autorités nationales par les canaux de coopération judiciaire internationaux⁵⁰.

L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) est constitué depuis mai 2000 en centre de compétences et de coordination où doivent se rencontrer "le ministère de la défense (Direction générale de la gendarmerie nationale) et le ministère de l'économie, des finances et de l'industrie (Direction générale des douanes et droits indirects et direction générale de la concurrence, de la consommation et de la répression des fraudes)." L'Office doit notamment "animer et (...) coordonner, au niveau national, la mise en oeuvre opérationnelle de la lutte contre les auteurs et complices d'infractions spécifiques à la criminalité liée aux technologies de l'information et de la communication", "procéder, à la demande de l'autorité judiciaire, à tous actes d'enquête et de travaux techniques d'investigations en assistance aux services chargés d'enquêtes de police judiciaire sur les infractions dont la commission est facilitée par ou liée à l'utilisation des technologies de

⁴⁹ Albanie, Croatie, Estonie, Hongrie, Lituanie, Macédoine, Roumanie, Slovénie.

⁵⁰ Marcel FAURE, audition du 27 avril 2004.

*l'information et de la communication*⁵¹." L'OCLCTIC apporte ainsi l'expertise de ses personnels en soutien à d'autres services en matière d'interprétation de données de connexion, d'analyse de disques durs saisis et perquisitionnés, etc.

L'OCLCTIC procède également au traitement des signalements de contenus pédo-pornographiques adressés par les internautes sur le site officiel www.internet-mineurs.gouv.fr. La création de ce site a été décidée par le Gouvernement lors du Conseil de Sécurité Intérieure du 13 novembre 2001, qui avait pour objectif de dégager les moyens d'une plus grande protection des enfants et d'une répression accrue des infractions à caractère sexuel dont ces derniers sont victimes. Une base de données regroupe l'ensemble des informations relatives aux sites signalés afin de disposer de toutes les informations nécessaires à l'engagement des poursuites et de rapprocher les informations issues de signalements ultérieurs. L'OCLCTIC peut demander à un prestataire ou à un juge de bloquer, ou informer un magistrat en vue de faire bloquer l'accès à des contenus hébergés en France. Il signale ces contenus au parquet de Paris ou informe les services d'Interpol lorsque les signalements concernent des matériels hébergés hors de France.

Les services territoriaux de la police judiciaire, placés auprès des Directions régionales de la police judiciaire (DRPJ) peuvent également intervenir, sur saisine d'un parquet ou de leur propre initiative. Ainsi la Brigade de protection des mineurs (BPM) de la Direction régionale de la police judiciaire (DRPJ) de Paris, dont la compétence territoriale couvre la région la plus "connectée" de France, qui est aussi la zone d'implantation des principaux fournisseurs d'accès à l'internet, a constitué un groupe de trois (2003), puis de six (2004) enquêteurs dont l'activité se concentre sur la recherche et la poursuite d'infractions impliquant l'utilisation des technologies de l'information. Au cours de sa première année d'existence, en 2003, ce groupe "Internet" a traité 96 affaires ayant trait dans leur grande majorité à la diffusion et à la détention de pédo-pornographie sur l'internet. A la date de leur audition, en mai 2004, les enquêteurs de la BPM prévoyaient de traiter plus de 300 dossiers en 2004⁵².

Avec le soutien de 50 enquêteurs spécialisés en criminalité informatique (ESCI) spécifiquement formés à la recherche d'infractions liées aux nouvelles technologies, les services de police locaux sont enfin également fondés à intervenir, d'autorité ou sur saisine du parquet, dans les affaires relevant de leur compétence territoriale.

Services de gendarmerie.

La Gendarmerie nationale intervient également dans la lutte contre la diffusion et la détention d'images pédo-pornographiques sur l'internet.

De compétence nationale, le département Internet du Service technique de recherches judiciaires et de documentation (STRJD) procède depuis 1998, d'initiative ou sur information des unités de la gendarmerie nationale ou de tiers ayant déposé un signalement sur l'adresse sitepj@gendarmerie.defense.gouv.fr, à la surveillance et à la recherche d'infractions sur les principaux protocoles de l'internet. C'est auprès de ce service qu'a été placé le Centre national d'analyse des images pédo-pornographiques (CNAIP), qui collecte depuis octobre 2003 l'ensemble des images recueillies par les différents services d'enquête français, en sorte d'opérer analyses et rapprochements permettant d'apporter une aide concrète aux enquêteurs de police et de gendarmerie. Ce

⁵¹ Décret n° 2000-405 du 15 mai 2000 portant création d'un office central de lutte contre la criminalité liée aux technologies de l'information et de la communication.

⁵² Marie LAJUS, Fabrice GAUTHIER, audition du 11 mai 2004.

service a récemment fait l'acquisition du logiciel *Image Seeker*, conçu par la société française LTU Technologies, qui facilite ces rapprochements.

Depuis 1992, le département informatique-électronique (INL) de l'Institut de recherche criminelle de la gendarmerie nationale (IRCGN) apporte un soutien technique (expertises, surveillance, interceptions) aux différents services de gendarmerie. Les examens scientifiques et les expertises conduites par l'IRCGN pour les enquêteurs et les magistrats ont porté, en 2003, sur plus de 2,4 téra-octets de données, dont plus de 80% étaient relatives à des affaires de pédophilie et de pédo-pornographie.

Avec le soutien de 80 personnels "NTECH" spécifiquement formés aux techniques d'enquête propres aux infractions liées aux nouvelles technologies, les différents services régionaux comme départementaux de gendarmerie sont également fondés à intervenir sur saisine et d'initiative. Comme on le notait plus haut, M. Philippe Jarlov, enquêteur de la section des Recherches de Bordeaux, détecte par exemple les serveurs de diffuseurs de contenus pédo-pornographiques basés dans toute la France à l'aide d'outils logiciels permettant l'automatisation de cette opération.

Freins à la poursuite et à la répression de la diffusion des contenus pédo-pornographiques.

Les services de police et de gendarmerie nationaux et, de plus en plus fréquemment, régionaux, regroupent de précieuses compétences. Le dispositif d'ensemble de répression de la diffusion de contenus pédo-pornographiques sur l'internet n'en paraît pas moins souffrir d'une grande complexité et du manque de moyens en personnels, en équipement et en capacités d'intervention.

La nécessaire évolution des moyens humains et matériels.

Les effectifs des services et groupes d'enquête spécialisés dans la répression des infractions commises par le vecteur des technologies de l'information n'ont pas évolué dans les mêmes proportions que le volume des dossiers relatifs à des cas de diffusion et de recel d'images pédo-pornographiques sur l'internet. Selon certains enquêteurs, le manque de moyens en personnels compétents, mais aussi en matériel et logiciels appropriés, fait aujourd'hui courir le risque que certains services d'enquête se trouvent contraints de privilégier la poursuite de certaines infractions plutôt que d'autres, ou ne soient pas en mesure d'atteindre certains objectifs, comme la recherche des mineurs victimes.

Le 7 septembre 2004, le ministre de l'Intérieur Dominique de Villepin, qui a fait de la lutte contre la cybercriminalité l'une de ses priorités, a annoncé un effort de formation d'enquêteurs de police et de gendarmerie spécialisés, dont l'effectif doit passer, à l'horizon 2007, à 300, puis 600. Au niveau national, les effectifs de l'OCLCTIC seraient amenés à passer de 38 à 75, et ceux de l'IRCGN de 30 à 50 gendarmes.

La relative dispersion des structures d'enquête.

L'analyse de l'organisation des services d'enquête permet de constater l'éclatement des unités de police et de gendarmerie, dont les actions à l'encontre des diffuseurs ou acquéreurs d'images pédo-pornographiques sur l'internet ne font l'objet d'aucune coordination systématique. Plusieurs services d'enquête, spécialisés ou non, locaux ou nationaux, de gendarmerie ou de police peuvent ainsi mener des enquêtes sur des faits identiques ou connexes, sans pour autant recouper et partager leurs informations et conclusions. Dans un domaine d'étendue et de compétence nationale, voire

internationale, on conçoit pourtant l'utilité d'un organisme central rassemblant tous les services concernés (police et gendarmerie, notamment) ayant mission de collecter toutes les informations relatives aux enquêtes en cours et d'assurer efficacement la coordination des unités spécialisées ou régionales en matière de lutte contre la pédo-pornographie sur l'internet.

Le ministre de l'Intérieur a annoncé son intention de procéder à la réorganisation des services de lutte contre les infractions liées aux technologies de l'information, le pôle de la gendarmerie étant dédié à la veille des contenus pédo-pornographiques et des activités pédophiles, et le pôle de la police nationale plus particulièrement aux faits de racisme, d'antisémitisme et de haine raciale, de terrorisme et de piratage informatique⁵³. Les modalités précises de cette réorganisation restent à préciser.

L'organisation territoriale des juridictions.

Chaque juridiction étant territorialement compétente, les affaires de diffusion ou de recel de matériels pédo-pornographiques sont susceptibles d'être traitées sans réelle coordination par une multitude de magistrats diversement formés. Certains magistrats et enquêteurs suggèrent ainsi que les compétences spécifiques à la répression de la cyber-criminalité pourraient être utilement renforcées, voire mutualisées, dans certaines juridictions⁵⁴.

Le parquet général près la Cour d'appel de Paris compte aujourd'hui de fait un magistrat spécialisé pour les affaires ayant trait aux technologies de l'information, auquel il y a lieu d'ajouter les neuf "magistrats référents" des parquets du ressort. Le parquet général près la Cour d'appel de Versailles a mis en place le même dispositif.

Les limites de la procédure pénale.

Examinant une affaire criminelle où un particulier, *"naviguant sur internet, a été choqué des découvertes qu'il a faites sur un site pédophile, et a voulu démasquer en se faisant passer pour un adolescent de 14 ans, les utilisateurs de ce site"*, la chambre criminelle de la Cour de Cassation a considéré, dans un arrêt du 1^{er} octobre 2003, qu' *"il ne peut être reproché un manque de loyauté à une personne physique qui veut, par un stratagème, empêcher de nuire les délinquants sexuels utilisant un site constitué sur des crimes commis à l'égard de jeunes enfants"*, admettant ainsi que l'on puisse recourir à une identité d'emprunt pour démasquer une infraction, pour autant qu'il n'y ait pas provocation à agir⁵⁵.

Il n'est toutefois pas certain que les enquêteurs soient pour autant légitimés à agir selon ces méthodes lorsqu'ils recherchent proactivement des diffuseurs de pédo-pornographie sur l'internet. Les enquêteurs ne peuvent de plus agir, aux fins de l'enquête, en *"coauteurs, complices ou receleurs"* des infractions ou de leurs produits, ni proposer une ou plusieurs images pédo-pornographiques aux animateurs de serveurs spécialisés, qui les exigent souvent avant d'autoriser l'accès d'internautes aux contenus illicites qu'ils distribuent. En l'absence de cadre légal spécifique, les enquêteurs recourant à une identité d'emprunt restent de plus susceptibles d'usurper l'identité d'un autre utilisateur de l'internet ou d'un service donné⁵⁶.

⁵³ Allocution de Dominique de VILLEPIN sur la lutte contre la cybercriminalité, 7 septembre 2004 - http://www.interieur.gouv.fr/rubriques/c/c1_le_ministre/c13_discours/2004_09_08_cybercriminalite.

⁵⁴ Yvon TALLEC, audition du 8 juin 2004.

⁵⁵ C. cass. crim., 1^{er} octobre 2003, 03-84142.

⁵⁶ L'usurpation d'identité devient un délit pénal dès l'instant où *"le fait de prendre le nom d'un tiers, [a été opéré] dans des circonstances qui ont déterminé ou auraient pu déterminer contre celui-ci des poursuites pénales"* (art. 434-23 du Code pénal). La condition, pour que le délit soit constitué, tient à ce qu'ait été pris *"le nom d'un tiers"*. A ce jour, il n'existe pas de jurisprudence qui puisse affirmer qu'emprunter un pseudonyme, une adresse IP ou une adresse de courrier électronique puisse être assimilable au *"nom"* évoqué dans l'article 434-23.

La loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité définit dans le Code de procédure pénale la notion d'infiltration et la procédure qui l'encadre : *"l'infiltration consiste, pour un officier ou un agent de police judiciaire spécialement habilité dans des conditions fixées par décret et agissant sous la responsabilité d'un officier de police judiciaire chargé de coordonner l'opération, à surveiller des personnes suspectées de commettre un crime ou un délit en se faisant passer, auprès de ces personnes, comme un de leurs coauteurs, complices ou receleurs⁵⁷."* A cette fin, l'agent infiltré peut recourir à une identité d'emprunt et, si nécessaire, acquérir, détenir, transporter, livrer ou délivrer des substances, biens, produits, documents ou informations tirés de la commission des infractions ou servant à leur commission, sans être tenu responsable de ces actes. Une telle procédure est aujourd'hui limitée aux enquêtes portant sur certains délits commis "en bande organisée", dont la liste limitative est définie à l'article 706-73 du Code de procédure pénale, et n'inclut pas la diffusion ou la détention d'images pédo-pornographiques. Certains enquêteurs souhaitent que ce procédé soit étendu à la recherche des contenus pédo-pornographiques et de leurs diffuseurs, afin de pouvoir démanteler plus facilement les réseaux d'échange de ces contenus.

Bon nombre d'enquêteurs soulignent enfin leur incapacité à constater la diffusion d'images pédo-pornographiques sur les sites dont l'accès est conditionné au paiement d'un droit d'accès par carte bancaire. Ils suggèrent que leurs moyens procéduraux et financiers soient étendus en sorte de pouvoir procéder, aux fins de l'enquête, à de telles opérations de paiement.

Introduit par la loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité, l'article 706-95 du Code de procédure pénale prévoit que *"si les nécessités de l'enquête de flagrance ou de l'enquête préliminaire relative à l'une des infractions entrant dans le champ d'application de l'article 706-73 [crimes et délits commis en bande organisée, dont sont exclues les atteintes aux mineurs et les infractions relatives à la pédo-pornographie] l'exigent, le juge des libertés et de la détention du tribunal de grande instance peut, à la requête du procureur de la République, autoriser l'interception, l'enregistrement et la transcription de correspondances émises par la voie des télécommunications selon les modalités prévues par les articles 100, deuxième alinéa, 100-1 et 100-3 à 100-7, pour une durée maximum de quinze jours, renouvelable une fois dans les mêmes conditions de forme et de durée. Ces opérations sont faites sous le contrôle du juge des libertés et de la détention."* Certains enquêteurs souhaitent que cette procédure spécifique puisse être étendue à la recherche d'infractions liées à l'échange d'images pédo-pornographiques et permette l'accès aux comptes de courrier électronique de suspects, ainsi qu'aux espaces de stockage de documents qui y sont fréquemment associés.

Ces propositions d'extension des moyens procéduraux des autorités policières, si elles renforceraient sans doute les capacités d'action des enquêteurs, n'en risquent pas moins de comporter des risques, notamment en matière de libertés publiques. Certains opposants à la loi du 9 mars 2004 craignent ainsi que les dispositions de ce texte ne soient appliquées abusivement, hors du cadre strict qui leur est imposées ou sans égard pour la gravité des faits suspectés ou poursuivis, et que le fait de rendre applicables les dispositions spéciales de la loi à l'enquête préliminaire en matière de recel de pornographie infantile n'ouvrent la voie à certains excès comme, par exemple, l'interception des communications électroniques et l'accès aux espaces de stockage en ligne de tous les correspondants identifiés d'un receleur avéré... Les bénéfices attendus de telles dispositions doivent ainsi être considérés au regard de la gravité du phénomène et de tels risques. Enfin, on peut se demander s'il est utile de procéder à l'extension des moyens de recherche des infractions sans que soient étendus dans le même temps les

⁵⁷ Loi n° 2004-204 du 9 mars 2004 art. 1. Code de procédure pénale, art. 706-81 et suivants.

moyens consacrés au traitement de ces dernières.

c. Moyens et limites de la coopération policière et judiciaire internationale⁵⁸.

Les législations dont se sont dotés un grand nombre d'Etats dans les années 1990 ne suffisent pas en elles-mêmes à remédier aux difficultés liées à l'accessibilité universelle des contenus sur l'internet. Les Etats doivent également se doter d'instruments de coopération policière et judiciaire adaptés à la poursuite d'infractions dans l'environnement ouvert qu'est l'internet.

Cette coopération peut contribuer à remplir certains objectifs intermédiaires ou finaux de l'action judiciaire que les autorités nationales ne peuvent atteindre seules : faire procéder au retrait de contenus illicites hébergés sur le territoire d'un autre Etat au vu d'une décision judiciaire française exécutoire, identifier le propriétaire, l'animateur ou un utilisateur d'un service en ligne, interpellé un suspect...

Les outils d'investigation à l'étranger et les instruments de la coopération policière.

La coopération policière internationale est régie par l'accès à des centres de ressources qui apportent une aide aux enquêteurs. Ces centres ont notamment pour finalité de coordonner l'action des services répressifs de plusieurs Etats et de leur apporter l'assistance utile en terme de rapprochement, de recherches et d'échanges d'informations. Ils sont notamment compétents en matière de traite des êtres humains, de pédo-pornographie et d'atteintes à la dignité humaine. Les centres ressources facilitent la lutte contre le crime et la délinquance en offrant leurs expertises aux services d'enquêtes. Des améliorations et des aménagements de leurs modes de fonctionnement paraissent toutefois encore nécessaires.

Interpol.

Le rôle de l'Organisation internationale de police criminelle (OIPC) Interpol consiste à coordonner l'action des polices des Etats membres, qui interviennent à la fois comme fournisseurs et demandeurs d'informations et de services. Interpol facilite également l'échange d'expérience et la définition de principes d'action communs, l'organisation de sessions de formation ou encore l'élaboration de guides des meilleures pratiques destinés aux services d'enquêtes.

La coopération s'applique à tous les types d'activité criminelle ou délictuelle qui présentent un caractère ou un élément international. Elle s'exerce spécialement dans les domaines de la criminalité de violence contre les personnes et la criminalité contre les biens. Interpol participe ainsi activement à la lutte contre l'exploitation sexuelle des enfants y compris sur l'internet.

Afin d'apporter un soutien immédiat aux enquêteurs chargés de mener des investigations sur une ou plusieurs infractions perpétrées sur ou au moyen de l'internet, et sous l'impulsion du G8, Interpol a décidé la mise en œuvre de points de contact fonctionnant 24 heures sur 24 et 7 jours sur 7 dans les services de police des Etats associés. En

⁵⁸ Myriam QUEMENER, sous-directrice de la justice pénale générale, et Joël FERRY, officier de liaison à la Direction des affaires criminelles et des grâces, ont largement contribué à la rédaction de cette partie. Qu'ils en soient remerciés.

France, c'est l'OCLCTIC qui remplit cette fonction. Interpol développe également des instruments nouveaux, comme une base de données centrale d'images pédo-pornographiques alimentée par tous les Etats membres et susceptible d'être interrogée à la demande de leurs autorités. Un tel outil permettra de rapprocher des informations et de participer plus efficacement à la lutte contre les crimes mettant en scène des mineurs. La France dispose au Centre national d'analyse des images pédo-pornographiques (CNAIP) d'un instrument de ce type, qui doit à présent monter en puissance.

En dépit de certains succès d'importance, comme le concours apporté par Interpol dans le cadre de l'opération "Cathédrale", au cours de laquelle 108 personnes ont été interpellées dans 13 Etats différents, dont la France, cette organisation comporte des limites : les enquêteurs font observer que les signalements et les informations transmis d'Etat à Etat par l'intermédiaire du secrétariat général d'Interpol transitent trop lentement et ne sont pas toujours suivis d'interventions des services de police destinataires des signalements. Ces signalements font surtout rarement l'objet d'une réponse : la "voie de retour" prévue par Interpol est peu exploitée.

Europol.

L'office européen de police - Europol, dont l'organisation et les missions sont prévues par la convention du 26 juillet 1995, est chargé du traitement des renseignements relatifs aux activités criminelles au sein de l'Union européenne (UE). Il constitue un point central de coordination et de coopération, chargé de soutenir les services enquêteurs afin de rationaliser leurs efforts et compléter leurs moyens en ce qui concerne la prévention et la lutte contre les formes graves de criminalité internationale organisée⁵⁹.

Europol peut ainsi faciliter les enquêtes relatives à des faits de diffusion et de recel de contenus pédo-pornographiques sur l'internet entre Etats européens. Il intervient en facilitant l'échange d'informations, en fournissant des analyses opérationnelles et stratégiques, en apportant son expertise et son assistance techniques aux enquêtes. Pour cela, il dispose d'un système d'informations qui n'a toutefois pas encore atteint sa pleine maturité. Cependant, les échanges directs et rapides de données peuvent également intervenir entre les officiers de liaison des Etats membres.

Les fichiers d'analyse enrichis des informations communiquées par les services d'enquête des Etats membres de l'Union européenne constituent aujourd'hui, d'après les enquêteurs, une plus-value au travail des enquêteurs pour combattre les réseaux criminels, examiner leur complexité et les diverses formes de leur manifestation. Un fichier d'analyse concernant la pédophilie sur Internet a été créé pour approfondir cette question. Un séminaire a été organisé sur ce thème en juin 2001 à La Haye. Enfin, en relation avec les services répressifs allemands, quatre séminaires de formation d'enquêteurs ont été organisés sur le thème de "la lutte contre l'exploitation sexuelle des enfants".

Pour traiter les dossiers, les services répressifs des Etats membres de l'Union européenne pourront constituer des équipes conjointes et mener des actions spécifiques d'enquête y compris des actions opérationnelles conjointes, comprenant en appui des représentants d'Europol.

Schengen.

Le 14 juin 1985, a été conclu à Schengen, un accord international visant, dans le cadre défini par l'acte unique européen, la création de l'espace communautaire sans frontière dénommé Schengen. Une convention signée le 19 juin 1990, complète cet accord et en

⁵⁹ Voir Alex Türk, *Quand les policiers succèdent aux diplomates*, Rapport d'information 523 (97-98), Paris, Sénat (Commission des lois), 1998.

précise les modalités d'application⁶⁰.

La coopération entre les Etats de l'Union européenne s'appuie aussi sur ce dispositif, qui définit le cadre de l'assistance mutuelle aux fins de la prévention et de la recherche de faits punissables, et permet l'intensification de la coopération policière dans les régions frontalières (article 39 de la convention)⁶¹. Le système d'information Schengen permet l'échange d'informations entre les Etats signataires et la consultation automatisée de données sur les personnes. Ces outils sont susceptibles d'être employés au profit de la répression de la diffusion et du recel d'images pédo-pornographiques entre Etats frontaliers signataires.

Les différents canaux de coopération policière au sein de l'Union européenne (Europol, Schengen) ne communiquent pas encore entre eux. Des discussions sont toutefois engagées pour permettre aux instances d'Europol d'accéder aux données contenues dans le système d'information Schengen⁶². La combinaison de ces outils dessine un cadre de coopération pertinent et semble pouvoir constituer un levier efficace dans la lutte contre la diffusion et le recel de contenus pédo-pornographiques sur le territoire de l'Union européenne, dont tous les membres punissent désormais ces comportements.

Au sein du G8 : le groupe de Lyon.

Le sous-groupe "haute technologie" du groupe de Lyon du G8 constitue enfin un lieu informel de réflexion et d'orientation des politiques de sécurité des Etats, dont l'influence n'est pas négligeable au sein des instances internationales. Il est à l'initiative de la base de données centrale d'images pédo-pornographiques mise en place par Interpol. La coopération renforcée des polices de Grande-Bretagne, des Etats-Unis, du Canada et d'Australie, y a ainsi été lancée en décembre 2003 sous la forme d'une *International Virtual Global Task Force* coordonnant les activités de certains services nationaux.

Il ressort de l'examen de la mise en œuvre des instruments existants que, si la coopération policière paraît se développer de manière satisfaisante aux niveaux global et européen en matière de lutte contre les contenus pédo-pornographiques sur l'internet, cette dernière n'est pas encore pleinement exploitée, et paraît encore largement entravée par le formalisme des procédures qui l'encadrent. Ainsi, de nombreux échanges d'informations entre enquêteurs ont encore lieu, en marge des procédures officielles, sur des bases informelles.

L'entraide judiciaire.

L'entraide judiciaire en matière pénale concerne la coopération entre les magistrats. Elle peut mener à l'extradition d'un ressortissant.

L'entraide judiciaire en matière pénale.

⁶⁰ La convention de Schengen concernera à terme tous les Etats de l'Union européenne. Pour l'heure, l'Islande a rejoint les Etats Schengen. En revanche le Royaume Uni et l'Irlande qui avaient refusé jusqu'à présent d'adhérer à l'accord préparent leur intégration pour septembre 2004.

⁶¹ A cela, il convient d'ajouter la possibilité pour les enquêteurs d'exercer un droit de suite (art 40 de la CASS) et d'observation (art 41 de la CASS)

⁶² Le parlement européen ne semble pas opposé à cette mesure. La commission des libertés, en a cependant fixé les limites : "le droit pour Europol d'utiliser le système de recherche du SIS devra être soumis au respect de certaines conditions de protection des données". Par ailleurs Europol ne pourra consulter que "les données qui se rapportent à l'objet pour lequel celles-ci ont été fournies et qui sont nécessaires à l'accomplissement de ses missions". La commission ajoute qu'"Europol ne doit pas pouvoir transmettre les données auxquelles il a accès à des Etats ou des organismes tiers".

Il existe une multiplicité de sources juridiques de l'entraide judiciaire en matière pénale. Celle-ci peut être réglée par des conventions bilatérales à l'exemple de la convention d'assistance juridique conclue entre la France et les Etats unis, des conventions multilatérales comme la convention européenne d'entraide judiciaire en matière pénale du 20 avril 1959 ou des conventions multilatérales spéciales comme la convention sur la cybercriminalité du conseil de l'Europe.

Lorsqu'il n'existe pas de convention, à la différence de certains Etats, la France présente les demandes des magistrats français à des autorités judiciaires étrangères en proposant, à titre de réciprocité, une offre identique dans des affaires comparables.

L'entraide judiciaire en matière pénale est par exemple réglée avec les Etats-Unis par un traité signé à Paris le 10 décembre 1998. Il est entré en vigueur le premier décembre 2001. C'est un instrument qui traite entre les deux pays de l'ensemble des questions liées à l'entraide judiciaire. Il n'est pas nécessaire que l'infraction poursuivie par l'un des deux Etats constitue également une infraction dans l'autre Etat pour mettre en œuvre les mesures d'entraide. Les dispositions de cet instrument s'appliquent à la cybercriminalité en général et à la lutte contre la pédo-pornographie en particulier en permettant notamment de recueillir sur le territoire de l'autre Etat toute image ou donnée relative à ce type d'infractions. L'instrument prévoit que l'entraide concerne tous les actes *"non prohibé par la législation de l'Etat requis"*. Les mécanismes particuliers d'entraide sont d'ailleurs visés dans le texte notamment les perquisitions, saisies et même les confiscations. Il arrive que dans le domaine de la pédo-pornographie, lorsque les serveurs sont implantés à l'étranger, certains Etats ne répondent pas à une demande d'entraide.

Il convient dès lors de rechercher au cas par cas l'existence de conventions liant la France avec d'autres Etats, et vérifier la nature de l'entraide qui y est visée.

En Europe, l'entraide judiciaire est réglée par une convention du Conseil de l'Europe du 20 avril 1959. Elle est matérialisée par un acte signé d'une autorité de justice qui demande à un homologue d'un autre pays de procéder à des mesures d'enquête pour l'affaire qu'elle instruit lorsque des investigations à l'étranger apparaissent nécessaires.

La Convention d'entraide de l'Union européenne signée le 29 mai 2000 vise à remédier aux principales difficultés de l'entraide judiciaire en assouplissant la gestion des dossiers et en introduisant un dialogue entre les parties afin d'éviter le blocage des demandes. Ainsi, les demandes d'entraide pourront être adressées directement de magistrat à magistrat sans passer par les administrations centrales, en utilisant éventuellement le courrier électronique. Les demandes d'entraide pourront être exécutées conformément aux procédures et aux formalités définies par l'Etat requérant. Il est prévu la possibilité de mettre en place des équipes communes d'enquête composées d'agents de services appartenant à plusieurs Etats. Le magistrat français pourra également procéder par vidéoconférence à l'audition d'un témoin, d'un expert ou de la personne poursuivie.

Mais cette convention, adoptée et signée par les quinze pays de l'Union européenne, doit encore être ratifiée par chacun des Etats de l'Union afin d'en inclure les principes dans le droit national des Etats et la rendre applicable. La ratification du texte par la France devrait intervenir très prochainement. La loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité prend déjà en compte certains principes de la convention dans un chapitre consacré aux dispositions concernant la lutte contre la délinquance et la criminalité internationale. Un chapitre intitulé *"de l'entraide judiciaire internationale"* vise à améliorer les échanges entre les Etats. Un chapitre particulier de la loi est enfin consacré à l'Union européenne et aux pouvoirs reconnus aux agents étrangers détachés auprès d'une équipe commune d'enquête.

Au delà de cette convention, d'autres dispositions, insufflées notamment par la convention d'application des accords de Schengen du 19 juin 1990, ont été adoptées en vue de favoriser l'entraide judiciaire. Il s'agit notamment de la simplification de la transmission des notifications d'actes de procédure et de certaines dénonciations d'infractions aux fins de poursuites entre les Etats parties, ainsi que de la transmission directe des demandes d'entraide judiciaire comme voie normale des échanges entre les autorités (article 53 de la convention). On ajoutera que l'article 31 du traité d'Amsterdam dispose que l'action en commun dans le domaine de la coopération judiciaire en matière pénale vise entre autres à faciliter l'extradition entre les Etats membres.

Enfin, la France a procédé avec d'autres Etats à l'échange de magistrats de liaison⁶³. La réussite de cette expérience, qui a déjà porté ses fruits en matière de recueil de certaines preuves dans le cadre notamment d'enquêtes sur l'exploitation sexuelle de mineurs, a conduit l'Union européenne à imaginer un réseau couvrant l'ensemble des Etats de l'Union et fonctionnant vingt-quatre heures sur vingt-quatre. Ce réseau a pour finalité de faciliter l'exécution des demandes d'entraide judiciaire relatives aux formes graves de criminalité, de coordonner les demandes d'enquêtes judiciaires et de fournir toutes les informations nécessaires aux magistrats de l'Union européenne sur les systèmes juridiques, les textes en vigueur et les règles de procédure.

Cependant, malgré ces outils et avancées, certaines demandes d'entraide ne sont pas traitées avec célérité, ou pas du tout. De telles situations peuvent résulter de difficultés administratives, mais également de l'impact politique du contenu des demandes.

Le régime de l'extradition.

La loi pénale française est applicable aux infractions commises sur le territoire de la République (art. 113-1 du code pénal). L'infraction est réputée commise sur le territoire de la République dès lors qu'un de ces faits constitutifs a eu lieu sur le territoire (art. 113-2 du code pénal). En outre, la loi pénale française est applicable aux crimes et délits punis d'une peine d'emprisonnement commis hors du territoire de la République par un français ou par un étranger lorsque la victime est française.

L'extradition est le moyen juridique pour un Etat requérant de réclamer d'un Etat requis la mise à disposition d'une personne afin de procéder à sa traduction devant une juridiction de jugement ou à l'exécution de sa peine. La France a ratifié la Convention européenne d'extradition du 13 décembre 1957. En l'absence de texte international applicable, le droit d'extradition français est réglé par la loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité, qui a introduit dans le code de procédure pénale un principe de réciprocité avec l'Etat concerné⁶⁴.

Parmi les principes majeurs applicables, pour qu'une extradition obtienne une réponse favorable, il est nécessaire que les faits reprochés soient considérés comme un crime dans la législation de l'Etat demandeur et dans la législation française, selon le principe de la double incrimination, ou réponde à un seuil minimum de gravité. L'extradition pourra ne pas être prononcée par un Etat à l'égard d'un de ses ressortissants. En outre, conformément aux bonnes pratiques adoptées par les Etats du G8, un pays refusant l'extradition pour des motifs de nationalité s'engage à soumettre l'affaire à ses autorités judiciaires nationales en vu d'engager des poursuites contre la personne mise en cause.

Le mandat d'arrêt européen se substitue, au sein de l'Union européenne, au processus de l'extradition.

⁶³ Tel est le cas avec les Pays Bas, l'Italie, l'Allemagne, l'Espagne, le Royaume Uni, et en dehors de l'Union européenne avec la République Tchèque et les Etats-Unis.

⁶⁴ Articles 696 à 696.24 et 696.34 à 696.41 du code de procédure pénale.

Le mandat d'arrêt européen.

Sur le plan de l'Union européenne, la décision-cadre⁶⁵ relative au mandat d'arrêt européen et aux procédures de remises entre Etats membres fait notamment référence à l'exploitation sexuelle des enfants, à la pédo-pornographie, et à la cybercriminalité. Dès lors que l'infraction est punie d'une peine de prison d'un maximum d'au moins trois ans, il n'est pas requis la double incrimination pour mettre à exécution ce mandat d'arrêt.

La loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité prévoit l'application en France du mandat d'arrêt européen et la levée de la double incrimination dans les affaires d'exploitation sexuelle des enfants et de pornographie infantile punies d'au moins trois ans d'emprisonnement :

« Art. 695-23. - L'exécution d'un mandat d'arrêt européen est également refusée si le fait faisant l'objet dudit mandat d'arrêt ne constitue pas une infraction au regard de la loi française.

« Par dérogation au premier alinéa, un mandat d'arrêt européen est exécuté sans contrôle de la double incrimination des faits reprochés lorsque les agissements considérés sont, aux termes de la loi de l'Etat membre d'émission, punis d'une peine privative de liberté d'une durée égale ou supérieure à trois ans d'emprisonnement ou d'une mesure de sûreté privative de liberté d'une durée similaire et entrent dans l'une des catégories d'infractions suivantes :

(...)

« - exploitation sexuelle des enfants et pornographie infantile

(...) »

Eurojust.

Intégré au traité de l'Union européenne par le conseil européen de Nice en décembre 2000, Eurojust est envisagé comme une unité de coopération opérationnelle de lutte contre la criminalité. Organe de l'Union européenne, il sera chargé de promouvoir et d'améliorer la coordination et la coopération entre les autorités judiciaires compétentes des Etats membres de l'Union européenne. Il pourra demander aux procureurs nationaux de faire procéder à une enquête ou d'engager des poursuites, de dénoncer des infractions aux autorités compétentes d'un autre Etat membre, de participer à la mise en place d'équipes communes d'enquête.

L'entraide judiciaire dans la Convention sur la cybercriminalité.

La Convention sur la cybercriminalité, signée à Budapest le 23 novembre 2001, est un instrument juridique majeur et inédit. Elle définit notamment des moyens et des axes de coopération internationale permettant de lutter plus efficacement contre la cybercriminalité.

La Convention établit des principes de base en matière de procédure afin de trouver et recueillir les preuves électroniques nécessaires à découvrir et poursuivre les auteurs d'infractions perpétrées au moyen des réseaux numériques. Ces mesures portent sur la conservation de données, la perquisition et la saisie informatique, la collecte de données de connexion et l'interception des communications.

Selon les termes de la Convention, les services d'enquêtes des Etats doivent s'unir et

⁶⁵ Décision-cadre 2002/584/JAI du Conseil, du 13 juin 2002, relative au mandat d'arrêt européen et aux procédures de remise entre Etats membres. Le 6^{ème} considérant indique qu'il s'agit de la première concrétisation du principe de reconnaissance mutuelle que le Conseil européen a qualifié de pierre angulaire de la coopération judiciaire. Le mandat d'arrêt européen s'applique entre les Etats de l'Union européenne qui ont transposé cette décision. Sur les vingt-cinq Etats de l'Union européenne, seule l'Italie n'a pas encore transposé ce dispositif.

s'entendre pour effectuer des actes d'enquête en lieu et place des services demandeurs et leur communiquer d'urgence les résultats obtenus. Aussi, en plus des formes traditionnelles d'entraide et d'extradition, la Convention propose de nouveaux moyens de procédure constituant une nouvelle forme d'entraide judiciaire. Par exemple, il pourra être procédé à une perquisition et saisie pour le compte d'un autre Etat, et toutes les informations utiles à l'enquête de l'Etat requérant devront être communiquées, notamment lorsque celles-ci ont transité par un Etat intermédiaire.

En matière d'extradition, la Convention dispose que si celle-ci est refusée sur la base de la nationalité de la personne recherchée ou parce que la partie requise s'estime compétente pour cette infraction, l'Etat requérant peut demander à l'Etat requis de soumettre l'affaire à ses propres autorités aux fins de poursuites et de lui rendre compte de l'issue de l'affaire.

Cet instrument juridique pourrait être considéré comme une norme de référence incontournable. Pourtant, force est de constater que depuis la signature de la Convention par trente trois pays européens, auxquels il faut ajouter les Etats-Unis, le Japon, le Canada et l'Afrique du sud, huit Etats seulement ont ratifié le texte.

Il ressort en conclusion qu'il existe une grande diversité de vecteurs d'entraide judiciaire en matière pénale, qui complexifie le choix de l'instrument le plus pertinent. Tout en reconnaissant le principe de la souveraineté des Etats, les conventions facilitent les demandes d'entraide, élargissent de proche en proche le périmètre de leur application et ainsi limitent les refus d'application de leurs dispositions. Ces vecteurs peuvent être mobilisés aux fins de la lutte contre la pornographie infantile sur l'internet. Toutefois, les délais inhérents au traitement de ces procédures internationales sont souvent dénoncés par les enquêteurs comme n'étant pas approprié au traitement d'affaires de pornographie infantile sur l'internet, où les contenus sont extrêmement mobiles, et les auteurs des infractions localisés dans une multitude de pays : il n'est pas rare, en dépit des différents canaux de coopération existants, qu'une commission rogatoire internationale transmise en vue d'obtenir l'identité du titulaire d'une adresse IP d'un FAI étranger nécessite de trois à quatre mois pour aboutir. Les réponses fournies sont parfois imprécises, ou peu exploitables. Il arrive également que des réponses ne parviennent jamais. Les délais nécessaires à la mise en œuvre des nouveaux canaux de coopération et le fait que certains Etats ne participent pas à cet effort semblent indiquer que les collaborations informelles continueront de se développer, en marge des procédures et des instances établies par les accords internationaux.

d. Analyse des responsabilités, obligations et initiatives des fournisseurs d'accès et de services en ligne.

Quelle responsabilité pour les acteurs de l'internet ?

L'article 9 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique prévoit, en transposition de la directive relative au commerce électronique du 8 juin 2000⁶⁶, que "les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne" soit, en premier lieu, les fournisseurs d'accès à l'internet (FAI), ne peuvent voir leur responsabilité civile ou pénale engagée que dans les cas où :

⁶⁶ Directive 2000/31/CE du Parlement européen et du Conseil 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.

- ils sont à l'origine de la demande de transmission litigieuse ;
- ou ils sélectionnent ou modifient les contenus faisant l'objet de la transmission.

Le législateur affirme également que les prestataires techniques ne sont soumis à aucune obligation générale de surveillance des informations qu'ils transmettent ou qu'ils stockent, mais que le juge conserve la possibilité d'imposer une telle mesure de surveillance, ciblée et temporaire (art. 6-I-7°).

Selon les termes de l'article 6 de la loi, les prestataires assurant le stockage de données sur l'internet, soit les prestataires d'hébergement et les acteurs associés à leur statut, *"ne peuvent voir leur responsabilité pénale engagée à raison des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de l'activité ou de l'information illicites ou si, dès le moment où elles en ont eu connaissance, elles ont agi promptement pour retirer ces informations ou en rendre l'accès impossible"*.

Dans sa décision n° 2004-496 DC du 10 juin 2004, le Conseil constitutionnel a émis sur ce point une réserve d'interprétation estimant que : *"ces dispositions ne sauraient avoir pour effet d'engager la responsabilité d'un hébergeur qui n'a pas retiré une information dénoncée comme illicite par un tiers si celle-ci ne présente pas manifestement un tel caractère ou si son retrait n'a pas été ordonné par un juge"*. Selon une explication de la réserve d'interprétation livrée en conférence de presse, le caractère manifestement illicite d'un contenu désigne avant tout les messages incitant à la haine raciale et les images pédo-pornographiques⁶⁷. Faisant écho aux dispositions prévues par les articles 808 et 809 du Nouveau Code de procédure civile, la loi rappelle enfin (art. 6-I-8°) que le juge peut prescrire aux hébergeurs ou, à défaut, aux fournisseurs d'accès, en référé ou sur requête, toute mesure propre à prévenir un dommage ou à faire cesser un dommage occasionné par un contenu en ligne, soit par exemple le retrait d'un contenu, ou le fait d'en rendre l'accès impossible.

En outre, la loi du 21 juin 2004 oblige les prestataires français d'hébergement, d'une part, à *"informer promptement les autorités publiques compétentes de toutes les activités illicites mentionnées à l'alinéa précédent [ayant trait, notamment, à la pédo-pornographie] qui leurs seraient signalées et qu'exerceraient les destinataires de leurs services"* et, d'autre part, à *"rendre publics les moyens qu'[ils] consacrent à la lutte contre ces activités illicites"* (loi du 21 juin 2004, art. 6, al. 7). Ces dispositions ont légalisé des pratiques largement répandues auprès des principaux prestataires d'hébergement français, qui informent les autorités et procèdent, lorsque les besoins de l'enquête le permettent, au retrait des contenus illicites.

Enfin, les fournisseurs d'accès et d'hébergement "grand public" membres de l'AFA ont élaboré et souscrit ensemble le 14 juin 2004, sous l'égide du ministre délégué à l'Industrie, une charte clarifiant les modalités par lesquelles elles se conformeront aux objectifs assignés par la loi. Les fournisseurs grand public d'hébergement et de services internet "fixe" se sont par exemple engagés à faciliter le signalement de contenus illicites aux entreprises qui les hébergeraient, aux services de police (Internet-mineurs.gouv.fr) ou au point de signalement opéré par l'AFA (Pointdecontact.net) *"sur tous les espaces communautaires, objets de leurs services d'hébergement – tels que les forums de discussion, "chats", salons –, sur les pages d'accueil de leurs services, et le cas échéant, sur les pages de listes de réponses des moteurs de recherche intégrés à leurs portails, de manière à ce que ces usagers puissent effectuer ce signalement d'un seul 'clic'"*, (art. 2) à *"porter promptement à l'information des autorités de police compétentes (...) l'existence d'un contenu en ligne visé à l'article 1 [de nature pédo-pornographique ou*

⁶⁷ Estelle DUMOUT, Jérôme THOREL, "LCEN: le Conseil constitutionnel censure l' 'amendement Devedjian'", Paris, ZDNet France, 15 juin 2004.

raciste] (...), signalé par les internautes" et à "agir promptement pour retirer ces contenus ou pour en rendre l'accès impossible conformément aux dispositions légales en vigueur" (art. 3)⁶⁸. Ce dernier engagement est de plus prévu par les clauses des conditions générales d'utilisation de la plupart des prestataires français d'hébergement qui, lorsqu'ils ne sont pas membres de l'AFA, ne se conforment toutefois pas tous aux engagements liés à la charte.

L'exception à l'obligation d'effacement des données de connexion.

L'article L 34-1 du Code des postes et des communications électroniques prévoit une obligation générale d'effacement des données de connexion et de trafic générées et stockées par les prestataires de services de communication en ligne. Il mentionne trois dérogations à cette obligation d'effacement pour les besoins de la facturation des prestations des opérateurs, pour les besoins de la sécurité de leurs réseaux, et pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales.

L'article L 39-3 du Code des postes et des communications électroniques punit ainsi d'un an d'emprisonnement et de 75 000 euros d'amende et de peines d'interdictions d'exercer le fait, pour un opérateur ou l'un de ses agents, "1° De ne pas procéder aux opérations tendant à effacer ou à rendre anonymes les données relatives aux communications (...)" et "2° De ne pas procéder à la conservation des données techniques dans les conditions où cette conservation est exigée par la loi".

L'article 6-II de la loi pour la confiance dans l'économie numérique du 24 juin 2004 renforce les moyens d'identifier les créateurs de tous types de contenus en disposant que les fournisseurs d'accès à des services de communication en ligne et les fournisseurs d'hébergement "détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires".

Les décrets d'application de ces dispositions, qui n'ont pas encore été adoptés mais ont fait l'objet de diverses consultations, doivent compléter le dispositif de conservation des données de connexion, essentiel à la recherche des auteurs d'infractions commises par le moyen des réseaux, et aujourd'hui diversement appliqué. La loi prévoit que ces décrets doivent fixer la durée de conservation des données de connexion et d'identification, ainsi que le spectre des données à conserver. Les modes de réquisition de ces données, les tarifs facturés par les opérateurs aux tribunaux pour chaque réquisition uniformisés et le mode de versement pourraient également être organisés par la voie réglementaire. Des groupes de travail communs à l'AFA et à la Direction Générale de la Police Nationale ont été créés pour améliorer les procédures. Les enquêteurs espèrent beaucoup de la régularisation de ce dispositif, qui pourrait selon eux permettre un traitement plus rapide de leurs réquisitions auprès des intermédiaires techniques.

Certains prestataires de services prennent une part active à la lutte contre la pédo-pornographie sur l'internet.

Comme on l'a vu, la Commission européenne a favorisé le développement dans chaque Etat membre de *hotlines* de signalement de contenus illicites. Ces points de signalement

⁶⁸ "Charte des prestataires de services d'hébergement en ligne et d'accès à Internet en matière de lutte contre certains contenus spécifiques", 14 juin 2004 - http://www.afa-france.com/actions/charte_internet.htm.

sont opérés par les professionnels du secteur et par des associations de défense des droits de l'enfant. Depuis 1998, le réseau InHope a fédéré seize *hotlines* européennes, et quatre sites d'assistance associés basés en Australie, aux Etats-Unis, en Corée du Sud et à Taiwan⁶⁹. Ce réseau facilite l'échange rapide d'informations entre les *hotlines* des pays où ont été signalés les contenus illicites, et les points de signalements des pays où ils sont localisés.

Sous réserve des particularités et de la législation locale de chaque *hotline*, lorsqu'un contenu en apparence pédo-pornographique est signalé à un point de contact du réseau InHope, et que ce dernier est compétent sur le territoire où est hébergé le contenu, le point de contact transfère le signalement au prestataire d'hébergement concerné ainsi qu'aux autorités nationales. Si le contenu est hébergé dans un pays représenté par un membre du réseau InHope, le point de contact le transmet à son homologue local. En France, l'Association des Fournisseurs d'Accès et de services internet (AFA) opère depuis 1997, à l'adresse Pointdecontact.net, un site de signalement à l'usage des internautes français.

Outre la mise en place de points de contact, d'autres réalisations peuvent être observées à l'étranger, comme l'initiative du fournisseur d'accès British Telecom intitulée "*Cleanfeed*". En concertation avec certaines associations de protection de l'enfance et le *Home Office*, le premier fournisseur d'accès à haut débit de Grande-Bretagne bloque depuis le 21 juin 2004 l'accès de ses abonnés à une liste de sites pédo-pornographiques compilée par l'association *Internet Watch Foundation*, par ailleurs point de signalement de contenus pédo-pornographiques membre du réseau InHope⁷⁰. Plutôt que d'empêcher la diffusion et l'échange de matériel pédo-pornographique, cette mesure a manifestement pour objectif de prévenir l'exposition, accidentelle ou non, aux plus accessibles de ces contenus. Soutenue par le Premier ministre britannique, elle doit faire l'objet, à partir de septembre 2004, d'une série de consultations au cours duquel sera discuté le principe de l'extension d'une telle initiative à d'autres fournisseurs d'accès⁷¹. British Telecom a annoncé, trois semaines après la mise en place de son système, avoir bloqué plus de 230 000 tentatives d'accès aux sites proscrits, et jusqu'à 20 000 requêtes par jour. Contestés par l'association des fournisseurs d'accès britanniques (ISPA UK), ces chiffres comprennent les tentatives d'accès multiples à certains contenus par un même utilisateur et les tentatives d'accès involontaires aux contenus proscrits.

Un débat sur la pertinence et l'utilité de cette initiative a pris corps en Grande-Bretagne. La légitimité d'un organisme privé comme l'*Internet Watch Foundation* à établir des "listes noires" de sites a été mise en cause. Le blocage des sites risque de surcroît, selon ses détracteurs, de provoquer le blocage de ressources licites stockées par d'autres entités sur de mêmes serveurs mutualisés.

Semblable débat s'est tenu aux Etats-Unis, où une loi de l'Etat de Pennsylvanie (*Statute 7330*) obligeait depuis 2002 les fournisseurs d'accès à l'internet à bloquer l'accès aux sites pédo-pornographiques qui leur étaient notifiés par le procureur de l'Etat. La loi a été jugée contraire au Premier amendement de la Constitution des Etats-Unis le 10 septembre 2004 par un tribunal fédéral, au motif que le blocage de l'accès à 400 sites pédo-pornographique occasionnait le blocage collatéral de plus d'un million de sites licites⁷².

Enfin, la plupart des fournisseurs d'accès français, européens, et même américains, ne relaient pas sur leurs serveurs l'ensemble des groupes de discussion sur Usenet

⁶⁹ La liste des membres du réseau InHope est accessible à l'adresse : <http://www.inhope.org/english/about/members.htm>.

⁷⁰ Martin BRIGHT, "BT puts block on child porn sites", *The Observer*, Manchester, 6 juin 2004.

⁷¹ Robert JACQUES, "Blair backs BT child porn prevention filter", *VNUNet.com*, 22 juillet 2004.

⁷² *Center for Democracy and Technology, American Civil Liberties Union, Platagenet, Inc. vs. Gerald J. Pappert. United States District Court for the Eastern District of Pennsylvania*, 10 septembre 2004.

(*newsgroups*) existants, certains d'entre eux étant notoirement spécifiquement dédiés à l'échange de matériels pédo-pornographiques. Cette mesure technique, si elle empêche l'accès du plus grand nombre aux *newsgroups* dédiés à l'échange de contenus illicites, ne permet toutefois pas d'éradiquer ces derniers, et un véritable marché de l'accès à ces *newsgroups* a vu le jour sur certains serveurs qui les répliquent sciemment, sans plus de considérations légales ni éthiques.

II. L'UTILISATION DE L'INTERNET AUX FINS DE PREPARER UNE ATTEINTE SEXUELLE SUR UN MINEUR

Une majorité de jeunes Français ont aujourd'hui accès à l'internet, depuis leur domicile ou à l'école, notamment. Et à mesure que se développent leurs usages du réseau, il apparaît de plus en plus nettement que les usages *interactifs* de l'internet sont ceux qu'ils prisent le plus. L'internet ouvre ainsi des perspectives nouvelles et sans précédent de communication et de libre expression pour les millions de jeunes utilisateurs du réseau.

Tandis que se développent et se banalisent les pratiques sociales des jeunes sur l'internet (retrouver ses copains sur messagerie instantanée après l'école, s'en faire de nouveaux dans un salon de discussion généraliste ou thématique, s'inventer un personnage sur ces espaces publics ou dans un jeu en réseau...), des personnes mal intentionnées ont pu étendre ou déplacer sur le réseau leur recherche de faveurs sexuelles auprès d'enfants, et utiliser l'internet pour préparer une atteinte ou une agression sexuelle, ou encore un viol sur un mineur.

L'internet n'est évidemment pas à l'origine de tels comportements. Il n'est pas non plus démontré qu'évoluer dans ce nouvel espace social soit plus périlleux que dans d'autres environnements. Certaines particularités de l'internet et de ses usages, toutefois, sont susceptibles d'être exploitées par des personnes déterminées à abuser sexuellement d'enfants : les espaces publics de l'internet spécifiquement destinés aux jeunes peuvent par exemple servir de moyen de contacter ces derniers directement et immédiatement, un internaute peut aisément maquiller son identité réelle sur ces espaces publics, certaines informations personnelles imprudemment diffusées sur le réseau sont également susceptibles d'être employées aux fins d'approcher un enfant.

1. Perceptions et réalités des risques associés à certains usages de l'internet.

a. Un objet d'inquiétude mal connu.

Plusieurs faits divers récents, en France et à l'étranger, témoignent des risques d'atteintes et agressions sexuelles ou de viols que peuvent encourir les mineurs à la suite de contacts établis sur l'internet. A défaut de veille systématique du phénomène, la mesure de ce dernier reste malaisée.

Dans ce domaine plus encore que dans celui de la diffusion de contenus pédopornographiques sur l'internet, on ne saurait produire d'éléments statistiques satisfaisants pour établir le panorama de l'utilisation de l'internet aux fins de commettre les faits d'atteinte ou d'agression sexuelle ou de viol sur mineurs. Rares sont les décisions de justice se rapportant à un viol ou une agression sexuelle sur un mineur résultant d'une mise en contact sur l'internet. Les statistiques du casier judiciaire font état, pour les années 1998 à 2002, d'une condamnation prononcée en 2000 sur le fondement du délit d'atteinte sexuelle sur un mineur de 15 ans par un majeur mis en contact avec la victime par un réseau de télécommunications. Les faits de corruption de mineur par une personne mise en contact avec la victime par un réseau de télécommunications ont donné lieu à deux condamnations en 2000 et 2001.

Le 23 novembre 2004, le tribunal de grande instance de Brest a condamné un homme de 47 ans à trois ans d'emprisonnement dont 18 mois de sursis avec mise à l'épreuve

assorti de suivi médico-psychologique pour avoir commis une atteinte sexuelle sur une mineure de 13 ans rencontrée sur l'internet. D'après l'avocate de la famille, l'auteur de l'atteinte "*menaçait de révéler à sa mère ce qu'elle faisait sur Internet. Elle s'est soumise à son agresseur, sans révolte, mais sans consentement*"⁷³. D'autres affaires seraient encore en cours d'instruction, et la presse se fait régulièrement l'écho de mises en examen de suspects d'agressions sexuelles, de viols ou encore de proxénétisme sur des mineurs rencontrés sur les espaces publics de l'internet. Selon M. Eric Freyssinet, le département INL de l'IRCGN a contribué au cours des 12 mois précédents à l'expertise de matériels informatiques liés à deux affaires de ce type⁷⁴. D'autres affaires de cette nature étaient déjà connues et ont été jugées suite à l'utilisation du Minitel par l'agresseur. En 2001, par exemple, le tribunal correctionnel de Villefranche-sur-Saône condamnait un homme à quatre ans de prison ferme pour corruption de mineur et atteinte sexuelle avec circonstance aggravante pour avoir eu des relations sexuelles avec un adolescent de 13 ans, qui avait répondu à une annonce sur un réseau Minitel de rencontres.

En Grande-Bretagne, où ces questions font l'objet d'une attention particulière de la presse et des pouvoirs publics, la première affaire connue de cette nature remonte à 2000. Patrick G., un homme de 33 ans, a établi un contact avec une jeune fille de 12 ans, et entretenu avec elle des échanges réguliers durant deux mois, avant de lui faire subir des atteintes sexuelles. L'homme a été condamné en octobre 2000 à cinq ans de réclusion pour atteinte sexuelle sur mineur et possession de pédo-pornographie. A plusieurs reprises, la presse britannique s'est également fait l'écho d'affaires dans lesquelles un suspect appréhendé sur les lieux du rendez-vous qu'il avait fixé à un enfant après des contacts suivis sur l'internet n'avait pu aboutir, faute d'incrimination spécifique⁷⁵. Le fait divers qui a vu, en 2003, une écolière britannique de 12 ans, Shevaun P., fuguer en compagnie d'un ancien soldat âgé de 31 ans rencontré sur l'internet, a fait le tour du monde.

En décembre 2003, le consultant de l'organisation NCH John Carr avait recensé dans la presse britannique 27 cas d'enfants ou de jeunes gens ayant rencontré un adulte suite à un contact en ligne, et ayant été victime d'un viol ou d'une atteinte sexuelle grave lors de cette rencontre. Les victimes identifiées étaient en majorité des filles âgées de 12 à 15 ans. L'étude de NCH affirme que, au-delà de ces cas connus, un grand nombre d'affaires ont pu n'être pas signalées aux autorités ou aux médias⁷⁶.

Ces éléments épars ne reflètent pas toute la réalité du phénomène, et ne sauraient à eux seuls exprimer une tendance. Seule une étude des comportements de certains pédophiles et du détail des affaires en cours d'instruction et des condamnations prononcées permettrait d'élaborer enfin un constat précis de la réalité de ces risques. Il serait nécessaire, pour que de tels outils servent à guider l'action publique, que le rôle de l'internet dans la préparation des infractions soit systématiquement consigné par les enquêteurs et les tribunaux, même lorsque l'utilisation du réseau n'intervient qu'à titre accessoire ou n'entre pas directement dans la commission de l'infraction condamnée.

La mise en place d'un Observatoire Nationale de l'Enfance en Danger (ONED) par la loi du 2 janvier 2004 relative à l'accueil et la protection de l'enfance est porteuse de promesses. L'Observatoire a pour missions l'amélioration de la connaissance du phénomène de maltraitance, le recueil et l'analyse des données chiffrées, l'identification des partenaires produisant des statistiques, la mise en cohérence des concepts et définitions, l'identification des secteurs non couverts par les producteurs de statistiques, des études et recherches concernant l'enfance maltraitée et la mise en cohérence des différentes informations. Il doit participer au réseau des Observatoires européens.

⁷³ Frédéric BARILLE, "Le pédophile chassait sur Internet". Brest, *Ouest-France*, mercredi 24 novembre 2004.

⁷⁴ Eric FREYSSINET, entretiens des 14 et 18 octobre 2004.

⁷⁵ Will GARDNER, *The Sexual Offences Bill: Progress and the Future*. Tackling Sexual Grooming conference, Londres, 29 septembre 2003.

⁷⁶ John CARR, *Child abuse, child pornography and the Internet*, Londres, NCH, 2004. p.3.

b. Les usages sociaux de l'internet et leurs risques.

On observe en France une forme de retard dans la connaissance des usages des jeunes utilisateurs de l'internet. L'agrégation d'éléments d'information rassemblés dans d'autres pays d'Europe permet toutefois de se forger une idée des pratiques des jeunes, et de leur exposition à des sollicitations de nature sexuelle sur l'internet susceptibles d'entrer dans la préparation d'atteintes sexuelles.

L'internet comme terrain d'expérimentation sociale.

Selon l'enquête du CREDOC sur "*la diffusion des technologies de l'information dans la société française*", publiée en novembre 2003, 72% des 12-17 ans disposaient en juin 2003 d'un accès à l'internet sur leurs lieux d'étude ou de travail, tandis que 40% étaient équipés à domicile d'une connexion à l'internet, dont 16% à haut débit.

55% des 12-17 ans usagers de l'internet considèrent que le réseau est "*un bon outil pour se faire des amis et entretenir des relations*". Ainsi la messagerie instantanée (48% des 12-17 ans connectés), l'échange de fichiers sur les réseaux peer-to-peer (P2P) (31%) et les jeux en réseau (35%, 15% des 12-17 ans n'ayant encore jamais joué en réseau ayant l'intention de le faire dans l'année) figurent-ils parmi les principaux usages de l'internet par les jeunes⁷⁷.

Les chercheurs du Réseau Education-Médias canadien considèrent également que la communication par courrier électronique, *chat*, messagerie instantanée fait partie des usages favoris des jeunes sur l'internet, et s'intègre désormais à la vie sociale de nombreux jeunes internautes. Ils apportent des précisions intéressantes sur ces pratiques, issues de séries d'entretiens avec de jeunes utilisateurs : au quotidien, et entre amis, la messagerie instantanée semble avoir la préférence des jeunes internautes ; le courrier électronique, plus formel, sert plus volontiers à communiquer avec un enseignant ou un parent éloigné ; le *chat*, enfin, constitue un véritable terrain d'expérimentation et d'exploration sociale. Les chercheurs nous enseignent que de nombreux jeunes Canadiens explorent ainsi les interactions sociales en testant, sous le couvert de plusieurs avatars, différents comportements, attitudes et pratiques⁷⁸.

En ligne comme hors ligne, les relations sociales comportent des "situations limites" et des risques inhérents aux intentions d'autres acteurs, qu'ils soient eux-mêmes mineurs ou bien adultes.

Sollicitations en ligne et rencontres physiques.

Une enquête réalisée dans le cadre du programme SAFT (*Safety, Awareness, Facts and Tools*), financée par l'Union européenne et portant sur un large échantillon d'internautes âgés de 9 à 16 ans du Danemark, de Suède, d'Islande, de Norvège et d'Irlande, indiquait

⁷⁷ Régis BIGOT, "La diffusion des technologies de l'information dans la société française", Enquête "Conditions de vie et Aspirations des Français", CREDOC, Paris, juin 2003.

⁷⁸ RÉSEAU EDUCATION-MÉDIAS, *Young Canadians in a Wired World* - Phase II. Focus Groups. Réseau Education-Médias, Ottawa, février 2004.

en mai 2003 qu'entre 19% (Irlande) et 39% (Norvège, Danemark) des enfants fréquentant les *chats* s'étaient vu proposer une rencontre physique. Entre 12% (Irlande) et 26% (Suède) du même échantillon ont rencontré une personne avec laquelle ils avaient établi un premier contact sur l'internet.

31% des 1 511 jeunes internautes Britanniques âgés de 9 à 19 ans interrogés dans le cadre de l'enquête *UK Children Go Online*, coordonnée par l'*Economic & Social Research Council* (ESRC)⁷⁹, ont reçu en ligne des sollicitations sexuelles non désirées dans le courant de l'année. L'enquête met en évidence le fait que 8% des jeunes se connectant au moins une fois par semaine ont rencontré "hors ligne" une personne connue sur l'internet. Parmi ces derniers, 5% n'avaient averti personne de leur intention de rencontrer leur correspondant. L'étude rapporte enfin que 48% des jeunes Britanniques interrogés craignent d'être "*contactés par des personnes dangereuses*".

Une vaste enquête entreprise aux Etats-Unis en 2000 par le *National Center for Missing and Exploited Kids* (NCMEC) indiquait que 19% des membres d'un panel de 1 501 utilisateurs de l'internet âgés de 10 à 17 ans avaient reçu des "sollicitations sexuelles" non désirées dans le courant de l'année, ces "sollicitations sexuelles" recouvrant un ensemble très large de réalités, soit des situations où quelqu'un tente de convaincre l'enfant de parler de sexe alors qu'il ne le souhaite pas, ou pose des questions intimes auxquelles l'enfant ne souhaite pas répondre, des situations où des personnes demandent à l'enfant de se livrer à des activités sexuelles auxquelles il ne souhaite pas s'adonner, des situations où des amitiés liées sur l'internet avec des adultes ont comporté des "ouvertures" sexuelles, et des invitations à s'enfuir émanant de correspondants sur l'internet. 3% des enfants interrogés avaient fait l'objet d'une sollicitation "agressive", impliquant une tentative de contact en personne, par téléphone, ou par courrier traditionnel⁸⁰.

Les sollicitations de nature sexuelle reçues en ligne par ces enfants n'émanent naturellement pas toutes d'adultes conscients de solliciter un mineur, mais fréquemment d'autres jeunes utilisateurs, qui accèdent de plus en plus précocement à des registres de langage et de relations fortement sexualisés. Les enfants employant de plus en plus souvent, et plus volontiers encore sous couvert de pseudonymat, certains codes que l'on croyait réservés aux adultes, les risques propres aux mises en contact sur l'internet sont rendus difficiles à apprécier, dans la mesure il est parfois très difficile de distinguer le langage et les intentions d'un autre jeune usager de celles d'un adulte mal intentionné. Dans 48% des cas de "sollicitations sexuelles" rapportées dans l'enquête du NCMEC, l'initiateur de la sollicitation paraissait être âgé de moins de 18 ans. Il semblait être un adulte, le plus souvent âgé de 18 à 25 ans, dans 24% des cas. Les enfants interrogés ne pouvaient déterminer l'âge de leur correspondant dans 27% des cas⁸¹. Comme le note la sociologue Céline Metton, "*Internet est (...) devenu un accompagnateur privilégié des premiers émois amoureux*", où "*les "accroches" souvent très crues des garçons effraient les filles*"⁸². De même, le professeur Philippe Jeammet, psychiatre, note que "*le pseudonymat permet aux jeunes de s'approcher de comportements et de matériels qui leurs sont défendus, avec le risque de se faire piéger en oubliant leurs prévenances. C'est ainsi que certains jeunes, garçons avant tout, n'hésitent pas à représenter leur nudité devant leur webcam*"⁸³.

⁷⁹ Sonia LIVINGSTONE, Magdalena BOBER, *UK Children Go Online. Surveying the experiences of young people and their parents*. Economic & Social Research Council, Londres, Juillet 2004.

⁸⁰ David FINKELHOR, Kimberly MITCHELL, Janis WOLAK, *Online Victimization: A Report on the Nation's Youth*, Washington DC, National Center for Missing & Exploited Children (NCMEC), juin 2000.

David FINKELHOR, Kimberly MITCHELL, Janis WOLAK, "Highlights of the Youth Internet Safety Survey", *OJJDP Fact Sheet*, Washington DC, U.S. Department of Justice, Office of Justice Programs, n°4, mars 2001.

⁸¹ David FINKELHOR, Kimberly MITCHELL, Janis WOLAK, *Online Victimization: A Report on the Nation's Youth*, op. cit.

⁸² Céline METTON, "Ils s'aiment par Internet", in *Informations sociales*, n°111, novembre 2003. Paris, Caisse National des Allocations Familiales. pp. 32-41.

⁸³ Philippe JEAMMET, audition du 6 juillet 2004.

Malgré l'apparence fort "libérée" des échanges en direct entre jeunes sur l'internet, ces derniers font toutefois le plus souvent preuve d'une prudente réserve. Céline Metton précise que *"lorsque le contact est bon, les dialogues sur le chat font office de prénégociation à une rencontre de visu. Les deux interlocuteurs s'échangent leurs coordonnées téléphoniques, et se fixent ensuite par téléphone un rendez-vous dans un lieu public. Le téléphone portable est le prolongement naturel du chat : il occupe une place centrale dans le processus de rencontre. Il permet d'abord une certaine protection et maintient la relation hors du contrôle parental"*⁸⁴.

En France, le protocole d'accord signé le 4 février 2004 entre l'institution du Défenseur des Enfants et le ministère de la Jeunesse, de l'Education nationale et de la Recherche, qui s'intègre dans la démarche de sécurisation des usages de l'internet entreprise par le ministère, crée la possibilité que le Défenseur *"soit chargé, en relation étroite avec les académies, de faire une typologie des agressions le plus fréquemment répertoriées"* au cours de l'utilisation du réseau à l'école. De cette veille pourraient émerger de nouveaux indicateurs des risques ressentis par les jeunes utilisateurs de l'internet à l'école.

Profils de victimes et méthodes de "prédateurs".

Psychiatres, enquêteurs, sociologues, ainsi que l'ensemble des observateurs des pratiques sociales des jeunes sur l'internet, notent que les adolescents constituent, parmi les mineurs, le groupe le plus exposé aux sollicitations de nature sexuelle de la part d'agresseurs potentiels sur le réseau. Les garçons, *"sexuellement curieux et inexpérimentés et un peu rebelles"*, sont d'après l'auteur d'un rapport du *National Center for Missing and Exploited Children* (NCMEC) et du ministère de la Justice américain, les plus susceptibles d'être les cibles d'adultes cherchant à obtenir les faveurs sexuelles d'enfants. Ce même auteur considère que les *"enfants de familles dysfonctionnelles et de familles où l'on communique peu encourent des risques significatifs de séduction"*⁸⁵. Le Professeur Jeammet confirme que les enfants les plus vulnérables sont, sur l'internet comme hors ligne, les plus menacés : si les enfants éprouvant des carences affectives importantes sont la plupart du temps très méfiants à l'encontre des adultes, ils font également preuve d'une grande candeur à l'égard des personnes qui gagnent leur confiance⁸⁶.

L'internet offre aux agresseurs potentiels de nouveaux moyens d'identifier une future victime, puis de tisser avec elle des liens et une intimité qui pourront résister, le cas échéant, à la révélation de l'âge véritable de l'adulte. John Carr décrit, pour l'organisation NCH, le mode opératoire typique d'un "prédateur" sur l'internet comme un processus méticuleux au cours duquel un pédophile va aborder un mineur dans un espace public de discussion en se présentant comme de quelques années plus jeunes que son correspondant, isoler l'enfant dans un salon de discussion particulier, puis gagner sa confiance au cours d'une relation dont il insistera pour qu'elle reste secrète, et qui pourra s'établir suivant plusieurs modes de communication : courriers électroniques, messagerie instantanée puis, parfois, téléphone et téléphone mobile⁸⁷. De la même façon, l'auteur du rapport du NCMEC décrit un processus s'inscrivant dans la durée. Il précise que les agresseurs sexuels déterminés à établir des relations sexuelles avec des enfants développent fréquemment des aptitudes particulières à identifier les enfants les plus

⁸⁴ Ibid.

⁸⁵ Kenneth V. LANNING, *Child Molesters: A Behavioral Analysis*. Washington DC, National Center for Missing & Exploited Children, Office of Juvenile Justice and Delinquency Prevention - U.S. Department of Justice, septembre 2001.

⁸⁶ Philippe JEAMMET, audition du 6 juillet 2004.

⁸⁷ John CARR, *Child abuse, child pornography and the Internet*, op. cit.

vulnérables et à s'identifier à leurs victimes : ils connaissent le plus souvent les derniers jeux vidéo, jouets, films, musiques ou sites *web* susceptibles d'intéresser les jeunes dont ils cherchent à gagner la confiance ; ils savent également séduire un enfant en dispensant à ce dernier attention, affection et cadeaux⁸⁸.

c. La question de la diffusion de données personnelles d'enfants.

Si le risque de contacts en ligne entre des enfants et des agresseurs potentiels s'exprime de manière particulièrement sensible sur les espaces interactifs (*chats*, notamment) car les protagonistes sont mis instantanément en contact, la publication sur le *web* de certaines informations personnelles peut, à l'évidence, être un facteur de risque en facilitant le rapprochement d'adultes et de mineurs.

Des associations de défense des droits de l'enfant expriment ainsi leurs inquiétudes au sujet de la diffusion de telles données personnelles sur des sites associatifs ou scolaires, par exemple, ou encore de services dédiés à faciliter les rencontres entre jeunes personnes. M. Alain Boulay, président de l'Association d'aide aux parents d'enfants victimes (APEV) recommande une plus grande prudence des organismes publiant les photographies, et parfois certaines informations nominatives précises sur les enfants (écoles, clubs sportifs), et appelle de ses vœux la diffusion d'une circulaire ministérielle sur le sujet⁸⁹. Le rappel des dispositions légales punissant la fixation, l'enregistrement et la transmission de l'image d'une personne sans son consentement ou celui de ses parents si elle est mineure, pourrait conduire de nombreux sites à régulariser les informations qu'ils rendent accessibles.

En Grande-Bretagne, le retrait des données nominatives relatives aux mineurs sur les sites *web* des écoles fait partie des recommandations aux établissements dans le cadre du plan d'équipement *National grid for learning (NGFL)* du secrétariat à l'Education⁹⁰. Et selon la *task force* "Protection des mineurs sur l'internet" du *Home office* britannique, "*les profils et les annuaires d'utilisateurs [de services de chat] peuvent permettre à une personne déterminée à abuser d'un mineur d'accéder à des informations très utiles, ainsi que d'établir un premier contact*"⁹¹. Diverses recommandations relatives à la préservation de l'anonymat des jeunes utilisateurs de l'internet ont été formulées parmi les "modèles de bonnes pratiques" élaborées en janvier 2003 par la *task force* "Protection des mineurs sur l'internet" du *Home office* britannique, qui comprend des représentants des pouvoirs publics, des acteurs économiques et des associations. Le ministère de l'Intérieur britannique recommande par exemple que "*les sites web procèdent avec prudence lorsqu'ils incluent des photographies, des coordonnées ou d'autres détails pouvant servir à identifier ou à contacter des enfants.*" Le *Home office* recommande également que les enfants soient encouragés à ne pas déclarer leurs adresse et numéro de téléphone lorsqu'ils remplissent leur "profil public" d'utilisateur d'un service en ligne, et qu'il leur soit possible de masquer un maximum d'informations⁹².

⁸⁸ Kenneth V. LANNING, *Child Molesters: A Behavioral Analysis*, op. cit.

⁸⁹ Alain BOULAY, audition du 1^{er} juin 2004.

⁹⁰ Voir : <http://safety.ngfl.gov.uk/>

⁹¹ HOME OFFICE TASK FORCE ON CHILD PROTECTION ON THE INTERNET, *Good practice models and guidance for the internet industry on: chat services, instant messaging (IM), web based services*. Londres, Home Office Communication Directorate, janvier 2003.

⁹² Voir : <http://www.homeoffice.gov.uk/crime/internetcrime/taskforce.html>. Le sous-groupe responsable de l'élaboration de ces recommandations compte des représentants des principales sociétés et associations professionnelles (AOL, BBC Online, ICSTIS, ISPA, LINX, Microsoft, Yahoo!, Surf Control...) et associations de protection des enfants (Childline, NCH, Childnet International...).

d. La relative ignorance des parents.

Différents indicateurs suggèrent qu'une minorité de parents sont aujourd'hui bien informés sur les risques qui peuvent être associés à certains usages de l'internet et aux moyens de les prévenir.

Un sondage "Eurobaromètre" de mars 2004, réalisé en novembre-décembre 2003 auprès de 16 000 citoyens de 15 Etats membres de l'Union, indique que 55% des parents français de jeunes utilisateurs de l'internet souhaitaient plus d'informations sur les moyens de sécuriser l'utilisation de l'internet par leurs enfants. 49% interdisent aux enfants de transmettre sur l'internet des informations personnelles les concernant. De même, 38% des parents utilisant régulièrement l'internet demandaient à leurs enfants de les informer de toute découverte déplaisante qu'ils pourraient faire en ligne. Et tandis que 39% interdisent à leurs enfants de rencontrer quiconque dont ils auraient fait la connaissance sur l'internet, 32% interdisent même à leurs enfants de fréquenter les *chat rooms* ou d'y communiquer avec des étrangers⁹³.

D'autres études mettent en évidence le fait que les parents n'ont pas encore pris, dans leur majorité, la mesure des risques pouvant être associés à certains usages de l'internet. Les résultats de la toute récente étude conduite sous l'égide de l'*Economic & Social Research Council* en Grande-Bretagne⁹⁴ indiquent ainsi que si 31% des jeunes utilisateurs de l'internet 9 à 19 ans interrogés reconnaissent avoir reçu des commentaires non désirés de nature sexuelle, 7% seulement des parents pensent qu'un tel événement s'est produit. De même, alors que 5% seulement des parents interrogés pensent que leurs enfants ont transmis des informations personnelles sur l'internet, près de la moitié (46%) des jeunes interrogés déclarent avoir déjà transmis à un correspondant rencontré un ligne leurs nom complet, leur âge, leur adresse électronique, leur numéro de téléphone, ou les coordonnées de leur école.

2. L'action des parties concernées et ses limites.

Méconnu, difficile à quantifier, le phénomène de l'utilisation de l'internet par des personnes mal intentionnées aux fins de commettre des atteintes sexuelles sur des mineurs fait également l'objet d'assez peu de mesures spécifiques de la part des acteurs engagés dans la protection de l'enfance sur le réseau.

a. Le cadre juridique et procédural en France et à l'étranger.

Le droit français n'incrimine pas spécifiquement le fait de rechercher les faveurs sexuelles d'un mineur.

Il n'existe pas, en droit français, d'infraction décrivant spécifiquement le fait de rechercher les faveurs sexuelles de mineurs, en ligne ou hors ligne, ou encore d'aller à la rencontre d'un mineur dans l'intention de commettre sur lui une atteinte ou agression sexuelle ou un viol.

⁹³ EUROPEAN UNION OPINION RESEARCH GROUP (EEIG), "Illegal and harmful content on the Internet", Special Eurobarometer 203/Wave 60.2, Bruxelles, Commission Européenne, mars 2004.

⁹⁴ Sonia LIVINGSTONE, Magdalena BOBER, *UK Children Go Online*, op. cit.

Seuls sont susceptibles d'être poursuivies l'agression sexuelle ou la tentative d'agression sexuelle (art. 222-27 à 222-31 du Code pénal), le viol ou la tentative de viol (art. 222-23 et 222-24 du Code pénal) sur mineurs, ainsi que l'atteinte sexuelle "*sans contrainte, menace ni surprise*" sur mineur de 15 ans (art. 227-25 et 227-26 du Code pénal) et les faits de proxénétisme (art. 225-7 et 225-7-1 du Code pénal). Le fait que le mineur victime ait été mis en contact avec l'auteur des faits ou que l'infraction ait été réalisée grâce à l'utilisation d'un réseau de télécommunications aggrave depuis la loi n° 98-468 du 17 juin 1998 les peines associées à ces crime et délits (art. 222-24 al. 8, 222-28 al. 6, 225-7 al. 10 et 227-26 al. 4 du Code pénal). Les incriminations existantes supposent donc que l'acte délictueux soit consommé ou que soit constaté un commencement d'exécution, soit "*des actes devant avoir pour conséquence directe et immédiate de consommer le crime, celui-ci étant ainsi entré dans la période d'exécution*"⁹⁵."

L'article 227-22 du Code pénal punit le fait de "*favoriser ou de tenter de favoriser la corruption d'un mineur*" soit, comme l'écrivait l'ancien Code pénal, d'exciter un mineur à la débauche. C'est pour lutter contre l'utilisation par certaines personnes des "*moyens modernes de communication, qui constituent d'indéniables progrès techniques, pour prendre dans leurs filets leurs futures victimes*"⁹⁶, que la loi du 17 juin 1998 a porté les peines punissant ce délit à un maximum de sept ans d'emprisonnement et 100 000 euros d'amende "*lorsque le mineur a été mis en contact avec l'auteur des faits grâce à l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un réseau de télécommunications*".

La jurisprudence pose toutefois quelques limites qui rendent délicat le recours à cet article pour punir la recherche de faveurs sexuelles auprès d'un enfant. La Cour de Cassation a ainsi jugé que "*l'excitation de mineurs à la débauche n'est pénalement punissable que si l'auteur des faits a eu en vue la perversion de la jeunesse, et non pas seulement la satisfaction de ses propres passions*"⁹⁷. La Chambre criminelle a toutefois également considéré que "*l'envoi de correspondances érotiques et de dessins pornographiques à un mineur*"⁹⁸ et le fait de pousser un mineur "*à un ou plusieurs actes d'immoralité par des conseils persistants et précis ou par des provocations réitérées*"⁹⁹ sont susceptibles d'être incriminés au titre de l'article 227-22 du Code pénal. Dans certaines circonstances, l'article 227-22 du Code pénal semble ainsi pouvoir fonder des enquêteurs informés de contacts répétés entre un mineur et un adulte à appréhender ce dernier avant qu'il ne commette l'une des atteintes décrites plus haut.

En Grande-Bretagne, le *Sexual Offence Act* de 2003¹⁰⁰ punit spécifiquement d'un maximum de 10 ans d'emprisonnement le fait, pour un adulte, de rencontrer ou d'aller à la rencontre d'un enfant de moins de 16 ans dans l'intention d'entretenir avec lui des relations sexuelles, et après avoir communiqué avec lui par quelque moyen que ce soit à au moins deux reprises. A l'évidence, l'intention des personnes susceptibles d'être poursuivies sur ce fondement sera difficile à établir. Il semble toutefois que la volonté du législateur britannique ait été de créer avant tout un outil de dissuasion à l'encontre d'agresseurs potentiels. On note que, soucieux de ne pas incriminer une simple intention, le législateur britannique a choisi de retenir pour élément matériel de l'infraction le fait de rencontrer ou d'aller à la rencontre du mineur.

La législation fédérale américaine rend également possible le fait d'appréhender et de poursuivre une personne avant qu'elle ne commette une infraction sexuelle sur un

⁹⁵ C. cass. crim. 25 oct. 1962 : *Bull. crim. N°292 (Lacour)* et n°292 (*Benamar et Schieb*).

⁹⁶ Elizabeth GUIGOU, garde des Sceaux, ministre de la Justice, discussion du projet de loi au Sénat le 28 octobre 1997 - http://www.senat.fr/seances/s199710/s19971028/s19971028_mono.html.

⁹⁷ C. cass. crim. 14 nov. 1990 : *Dr. Pénal* 1991.105.

⁹⁸ C. cass. crim. 25 janv. 1983 : *Bull. crim. N°29* ; *RS crim.* 1983. 668, obs. Levasseur.

⁹⁹ Dijon, 15 janv. 1954 : *Gaz. Pal.* 1954. 1. 224.

¹⁰⁰ *Sexual Offence Act* 2003, Section 15.

mineur. Ainsi quiconque convainc ou essaye de convaincre, de persuader ou de contraindre, par courrier ou tout autre moyen, un mineur de moins de 18 ans à participer à une activité sexuelle s'expose à une amende et jusqu'à quinze années de réclusion¹⁰¹. Certaines juridictions locales américaines prévoient spécifiquement l'utilisation d'un ordinateur pour solliciter un mineur. Cette disposition est à rapprocher de la conduite d'opérations de police "sous couverture" dans les *chat rooms*, où des enquêteurs disposent des moyens légaux de se faire passer pour mineurs et de constater des infractions. D'après une étude américaine, le constat de telles sollicitations de mineurs par des enquêteurs "sous couverture" a donné lieu, entre juillet 2001 et juillet 2002, à 644 arrestations¹⁰².

Les coopérations qui se sont développées entre pays anglo-saxons en matière de lutte contre la cybercriminalité doivent aboutir à la création prochaine d'équipes de surveillance issues des équipes spécialisées des autorités britanniques, américaines, canadiennes et australiennes, qui parcourront les salons de discussion du monde entier et établiront une présence visible des autorités sur ces espaces¹⁰³.

Procédés et limites de l'action des services d'enquête en France.

La nouveauté des situations auxquelles sont confrontés les enquêteurs et l'absence d'infraction décrivant spécifiquement le fait de rechercher les faveurs sexuelles de mineurs en ligne ou hors ligne amènent les services d'enquête à explorer des méthodes nouvelles de surveillance des espaces de discussion en ligne, et à souhaiter que le cadre de certaines procédures soit élargi. La création de nouvelles infractions et l'extension de procédures particulières constituent des actions de très large portée dont les bénéfices attendus doivent toutefois être mesurés et confrontés à la réalité des phénomènes qu'elles entendent combattre et aux risques qu'elles feraient peser sur les libertés publiques.

Certains services d'enquête français entreprennent de surveiller les espaces de discussion de l'internet où des enquêteurs, sous des identités fictives, sont à même d'observer le comportement d'adultes présumés en quête de faveurs sexuelles auprès de mineurs. On pourra opposer que cette méthode s'apparente à un procédé de provocation dès lors que l'enquêteur interagit directement avec un suspect.

Une enquête préliminaire peut être diligentée sous le contrôle du parquet sur le fondement des articles 227-24 (diffusion d'un message à caractère pornographique lorsque ce message est susceptible d'être perçu par un mineur) ou 227-22 (corruption de mineurs) du Code pénal, lorsqu'un mineur victime de telles sollicitations est connu. Les protagonistes pourront être identifiés par voie de réquisitions au cours de cette enquête préliminaire. L'infraction pourra être requalifiée au besoin si l'enquête apporte des éléments tendant à indiquer qu'une atteinte, une agression ou un viol a été commis sur une personne mineure.

Désireux d'intervenir en amont des faits, et convaincus que l'internet peut servir de vecteur de rencontres et de contacts entre des mineurs et des adultes déterminés à

¹⁰¹ "b) Whoever, using the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States knowingly persuades, induces, entices, or coerces any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempts to do so, shall be fined under this title, imprisoned not more than 15 years, or both" - 18 U.S.C. 2422: Coercion and Enticement.

¹⁰² Janis WOLAK, Kimberly MITCHELL, David FINKELHOR, *Internet Sex Crimes Against Minors: The Response of Law Enforcement*, Washington DC, National Center for Missing & Exploited Children (NCMEC), novembre 2003.

¹⁰³ "Cyber-cops to patrol Internet chatrooms", *CNN*, 9 juin 2004.

recueillir de ces derniers des faveurs sexuelles, certains enquêteurs souhaitent que puisse être incriminé spécifiquement le fait, pour un majeur, d'émettre une proposition de nature sexuelle à destination d'une personne connue comme mineure, l'utilisation de l'internet pouvant constituer une circonstance aggravante de la sanction prévue.

Certains enquêteurs souhaitent également que la procédure particulière en matière d'interceptions prévue par la loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité, puisse être étendue à la recherche d'infractions sexuelles à l'encontre de mineurs, et permette l'accès, au cours de l'enquête préliminaire, aux comptes de courrier électronique et la surveillance de l'activité dans les salons de discussion privés de personnes sur lesquelles reposent de fortes présomptions. L'article 706-95 du Code de procédure pénale prévoit que *"si les nécessités de l'enquête de flagrance ou de l'enquête préliminaire relative à l'une des infractions entrant dans le champ d'application de l'article 706-73 l'exigent [crimes et délits commis en bande organisée, notamment relatifs à la traite des êtres humains, ne comprenant pas spécifiquement les atteintes aux mineurs et les infractions relatives à la pédopornographie], le juge des libertés et de la détention du tribunal de grande instance peut, à la requête du procureur de la République, autoriser l'interception, l'enregistrement et la transcription de correspondances émises par la voie des télécommunications selon les modalités prévues par les articles 100, deuxième alinéa, 100-1 et 100-3 à 100-7, pour une durée maximum de quinze jours, renouvelable une fois dans les mêmes conditions de forme et de durée. Ces opérations sont faites sous le contrôle du juge des libertés et de la détention"*.

b. Rappel des responsabilités et initiatives des fournisseurs de services.

Le régime juridique applicable aux intermédiaires techniques et aux exploitants de services interactifs.

Le 14 octobre 2003, la direction du portail MSN décidait de fermer tous ses espaces de discussion gratuits dans le monde, sauf en Amérique du Nord et au Japon, où ces services sont devenus payants. Malgré la surveillance opérée par des employés et des bénévoles sur les *chats* du portail, les *chats* comportaient, selon Grégory Salinger, directeur de MSN France, *"des risques très importants liés à la pédophilie"*¹⁰⁴, entre autres abus. Cet événement invite à aborder l'examen du régime légal de responsabilité et des initiatives protectrices des éditeurs de services en ligne et des opérateurs de communications électroniques.

Comme on l'a rappelé plus haut¹⁰⁵, la loi du 21 juin 2004 pour la confiance dans l'économie numérique prévoit un principe général d'exonération de la responsabilité civile et pénale à raison des contenus accessibles sur les réseaux pour les *"personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne"*. Le législateur a également affirmé que les prestataires techniques ne sont soumis à aucune obligation générale de surveillance des informations qu'ils transmettent ou qu'ils stockent.

Les prestataires assurant le stockage de données sur l'internet *"ne peuvent voir leur responsabilité pénale engagée à raison des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de l'activité"*

¹⁰⁴ Arnaud DEVILLARD, "MSN ferme ses salons pour cause de dérive pornographique", *01Net*, 24 septembre 2003.

¹⁰⁵ Voir I / 2 / d. "Responsabilité, obligations et initiatives des fournisseurs d'accès et de services en ligne."

ou de l'information illicites ou si, dès le moment où elles en ont eu connaissance, elles ont agi promptement pour retirer ces informations ou en rendre l'accès impossible".

L'obligation de conservation des données d'identification.

Comme il a été exposé plus tôt, les fournisseurs d'accès et les fournisseurs d'hébergement sont tenus de conserver certaines données permettant l'identification des utilisateurs de leurs services dans le cadre d'une enquête judiciaire¹⁰⁶.

Le statut des fournisseurs de services de communication synchrone (*chats*) et asynchrone (*forums*) mérite d'être précisé. En tant que fournisseurs de services de la société de l'information permettant à des tiers de communiquer entre eux, ils sont susceptibles de relever de la définition de l'article 6.I.2 de la loi du 24 juin 2004 sur la confiance dans l'économie numérique, et d'être ainsi contraints de détenir et de conserver les données d'identification visées par l'article 6.II.

Les bonnes pratiques des fournisseurs de services.

Certains exploitants d'espaces publics de discussion synchrones (*chats*) ou asynchrones (*forums*, par exemple) affichent, dans ces espaces, des messages destinés à mettre en garde leurs jeunes utilisateurs contre les intentions de certains adultes ou encore un bouton permettant d'alerter les animateurs du service d'un comportement ou d'un contenu déplacés. D'autres entretiennent des équipes de modération ou de surveillance de ces espaces, où des surveillants le plus souvent bénévoles ont pour mission d'assister les utilisateurs et de surveiller les espaces de discussion en semonçant ou "bannissant" au besoin certains usagers peu respectueux de la loi ou des chartes d'utilisation associées aux services.

Les fournisseurs d'accès et d'hébergement "grand public" membres de l'Association des fournisseurs d'accès et de services internet (AFA) se sont engagés par une charte, le 14 juin 2004, à établir des liens vers "un formulaire de signalement d'abus" permettant aux utilisateurs "de signaler directement au prestataire du service d'hébergement concerné, ou au Point de contact de la profession accessible à l'adresse www.pointdecontact.net, ou aux autorités publiques dûment habilitées, tout contenu en ligne visé par [ladite] Charte". Ces liens ont vocation à être placés "sur tous les espaces communautaires, objets de leurs services d'hébergement – tels que les forums de discussion, "chats", salons –, sur les pages d'accueil de leurs services, et le cas échéant, sur les pages de listes de réponses des moteurs de recherche intégrés à leurs portails, de manière à ce que ces usagers puissent effectuer ce signalement d'un seul « clic »" (art. 2). Le principe d'une uniformisation des moyens de signalements, identifiés au besoin sur tous les espaces publics de discussion par une signalétique particulière et accompagnés d'explications visant à sensibiliser les enfants aux spécificités et aux règles des usages de l'internet, paraît une initiative prometteuse. Elle s'ajoute au dispositif d'information spécifique à la protection de l'enfance adopté par l'AFA, tendant à généraliser un lien "Protection de l'enfance" sur les pages d'accueil des sites de ses membres.

De nombreux espaces interactifs de l'internet font l'objet d'une veille par des modérateurs chargés, le plus souvent, de rappeler les règles de courtoisie aux

¹⁰⁶ Voir I / 2 / d. "Analyse des responsabilités, obligations et initiatives des fournisseurs d'accès et de services en ligne."

utilisateurs de l'espace (*chat* ou forum). Des applications fort populaires de l'internet, toutefois, ne peuvent être modérées ou surveillées. Ainsi, la grande majorité des *chats* comportent une partie publique, parfois surveillée, mais autorisent aussi une forme de communication de personne à personne échappant à la surveillance des modérateurs et des autorités. De même les dialogues échangés par l'intermédiaire des outils de messagerie instantanée ne sont pas susceptibles de surveillance hors du cadre des interceptions de correspondances.

c. Initiatives publiques et privées de sensibilisation des jeunes utilisateurs de l'internet, des éducateurs et des familles.

Diverses initiatives d'origines publiques ou privées entreprennent de sensibiliser les jeunes utilisateurs de l'internet aux risques qui peuvent être associés à certaines pratiques.

Les attentes des utilisateurs.

Le sondage "Eurobaromètre" de mars 2004 consacré aux contenus illégaux et préjudiciables sur l'internet nous renseigne sur les attentes des parents de jeunes utilisateurs de l'internet en matière de sensibilisation au bon usage de l'internet. 48% des parents interrogés dans les quinze pays membres de l'Union européenne entre novembre et décembre 2003 et dont les enfants utilisent l'internet souhaitent plus d'information sur les moyens de protéger leurs enfants des contenus illégaux et préjudiciables sur le réseau. En France, 55% des parents de jeunes utilisateurs de l'internet souhaitent plus d'informations.

Pour 47% des parents dont les enfants utilisent l'internet, l'école est la première source dont ils attendent que vienne l'information sur les moyens de sécuriser les usages de l'internet, avant les médias (32% : télévision, radio, journaux), puis les fournisseurs de services d'accès à l'internet et de télécommunications (28%) et le gouvernement ou les autorités locales (20%).

Il semble également que les parents interrogés préféreraient recevoir cette information par les canaux traditionnels plutôt que devoir la rechercher : à la télévision (43%), par courrier (43%) et, dans une moindre mesure, par les journaux (31%). Moins de 15% des parents souhaitant disposer de plus d'information sur les moyens de sécuriser les usages de l'internet préféreraient trouver cette information sur un site *web*¹⁰⁷.

La diversité des initiatives de sensibilisation en Europe et dans le monde.

On note, parmi les actions de sensibilisation et d'éducation à l'internet et à ses dangers potentiels, deux principaux types d'approches :

- l'énoncé de recommandations établies par des experts, destinées à sensibiliser les adultes ou les jeunes, et à leur indiquer les comportements jugés adéquats face à des situations potentiellement dangereuses sur l'internet ;

¹⁰⁷ EUROPEAN UNION OPINION RESEARCH GROUP (EEIG), "Illegal and harmful content on the Internet", op.cit.

- des démarches d'éducation aux médias, souvent reprises en Europe sous le terme "*Internet literacy*", à visée plutôt préventive, destinées à faire mieux connaître Internet aux adultes et aux jeunes (ses caractéristiques, ses fonctionnements, ses richesses, ses limites) de manière à les rendre autonomes et responsables dans leurs choix face à l'internet. Cette approche, plus exigeante et agissant sur le plus long terme, part des connaissances et des comportements réels des adultes et des jeunes et permet notamment de prendre en compte les évolutions rapides des technologies.

Incitations et financements européens.

Le rapport d'évaluation concernant l'application de la Recommandation du Conseil de l'Europe du 24 septembre 1998 sur la protection des mineurs et de la dignité humaine notait, en 2001, que "*des campagnes en vue d'une utilisation plus sûre d'Internet ont eu lieu dans la plupart des États membres*¹⁰⁸. *Plusieurs États membres ont souligné l'importance que revêtent les écoles en tant que lieu approprié pour des mesures pédagogiques*¹⁰⁹. " Depuis, les initiatives se sont multipliées, le plus souvent à l'initiative de la société civile, associations et acteurs économiques, parfois soutenus par la Commission européenne et les Etats. Récemment reconduit pour les années 2004-2008¹¹⁰, le "Programme d'action pour un internet plus sûr" (*Safer Internet Action Plan*) de la Commission européenne distribue 11,7 millions d'euros suivant huit lignes de projets réparties au gré des trois objectifs principaux du programme, parmi lesquels la mise en place de campagnes nationales de sensibilisation¹¹¹. Douze projets de sensibilisation aux risques liés aux usages de l'internet ont été financés dans ce cadre¹¹². La Commission prépare un projet de proposition d'extension du Plan d'action pour un internet plus sûr aux années 2005-2008.

Exemples d'initiatives gouvernementales.

Certains Etats ont choisi de développer des campagnes d'ampleur nationale. La *task force* dédiée à la protection des enfants sur l'internet du *Home Office* britannique est à l'origine, depuis 2002, de plusieurs initiatives de communication nationales, comme le site *thinkuknow.co.uk*, ou "*comment rester en sécurité tout en s'amusant sur l'internet*¹¹³", conçu à l'attention des enfants et de leurs parents. Début 2003, le gouvernement britannique a investi plus de 1,5 million d'euros dans une campagne pluri-médias (une campagne télévisée a été diffusée en juillet 2003) alertant enfants et parents sur les mesures de prudence élémentaires à adopter sur l'internet en général, et sur les *chats* en particulier¹¹⁴. Le *Home Office* a annoncé le 4 octobre 2004 l'extension jusqu'en janvier 2005 de cette campagne, qui fait l'objet de nouvelles annonces radiophoniques et de publicités en ligne. Plus de 450 000 euros seront investis par le Gouvernement britannique dans cette nouvelle phase¹¹⁵.

108 Autriche, Belgique, Allemagne, Grèce, Espagne, Irlande, Pays-Bas, Luxembourg, Suède, Finlande, Royaume-Uni. La France, avec le programme Educaunet, s'est également engagée dans cette voie en coopération avec une institution belge.

109 COMMISSION EUROPEENNE, Rapport d'évaluation de la Commission au Conseil et au Parlement européen concernant l'application de la recommandation du Conseil du 24 septembre 1998 sur la protection des mineurs et de la dignité humaine, op.cit., p.9.

110 Décision n° 1151/2003/EC du Parlement européen et du Conseil.

111 "Appel à propositions pour des actions indirectes au titre du plan d'action communautaire pluriannuel sur la promotion d'une utilisation plus sûre d'internet et des nouvelles technologies en ligne (2003 à 2004)", *Journal officiel de l'Union européenne*, C 209/30, 4 septembre 2003.

112 Tous ces projets peuvent être consultés sur le site du programme à l'adresse : http://europa.eu.int/information_society/programmes/iap/projects/index_en.htm et <http://www.saferinternet.org/projects/>.

113 Voir : <http://www.thinkuknow.co.uk/>.

114 "Online child safety drive launched", *BBC News - World Edition*, 6 janvier 2003.

115 HOME OFFICE, "Protecting children online when they are most at risk - new radio & online advertising", Communiqué de presse. Reference: 310/2004. 4 octobre 2004 - http://www.homeoffice.gov.uk/n_story.asp?item_id=1092.

Exemples d'initiatives de la société civile.

Différentes organisations à but non lucratif ont également entrepris de communiquer des conseils de prudence auprès des parents et des enfants, le plus souvent sur le *web*, qui constitue naturellement l'un des canaux de communication les plus économiques, même s'il n'est pas toujours le plus efficace. Pionnier de l'éducation aux médias, le Réseau Education-Médias canadien a par exemple créé le site *WebAverti*, qui multiplie les conseils de sécurité à l'attention des enfants de cinq tranches d'âges différentes, et met en valeur les moyens de "tirer le meilleur d'internet" autant que les dangers du réseau¹¹⁶. Aux Etats-Unis, l'*Internet Education Foundation (IEF)* a fédéré dès 1999 les principaux acteurs économiques de l'internet (constructeurs de matériel, opérateurs de réseaux, éditeurs de logiciels, éditeurs de services, sites marchands...) autour du site *GetNetWise*, qui constitue l'une des sources les plus complètes et les plus fréquentées en matière de sensibilisation à des usages raisonnés de l'internet¹¹⁷.

Certains acteurs économiques se sont également impliqués exclusivement dans la réalisation de sites et de documents attirant l'attention des plus jeunes et de leurs parents sur le bon usage de l'internet. La société Microsoft est ainsi à l'initiative, en Grande-Bretagne, du site *WebSafeCrackerz*, qui entreprend de sensibiliser sur un ton ludique les jeunes internautes à certains usages à risques de l'internet¹¹⁸.

Un autre "retard français" en matière d'éducation aux usages de l'internet ?

Les précédents travaux du Forum des droits sur l'internet portant sur la protection de l'enfance sur l'internet recensaient certains des projets paraissant les plus aboutis en ce domaine¹¹⁹.

La lente maturation des programmes de sensibilisation aux usages de l'internet à l'école.

On y notait la faiblesse des programmes de sensibilisation aux usages de l'internet à l'école en France, où le ministère de la Jeunesse, de l'Education nationale et de la Recherche s'est pourtant fixé pour objectif de développer la sécurité des jeunes utilisateurs sur les réseaux. Le ministre délégué à l'Enseignement scolaire a ainsi écrit aux recteurs d'académie au début de l'année 2004 qu'il souhaitait que des "*mesures de sensibilisation, de formation et de responsabilisation des utilisateurs*" accompagnent le renforcement des contrôles sur les contenus accessibles en ligne depuis les établissements scolaires : "*des actions d'information et de sensibilisation à destination des équipes éducatives et des élèves sont à prévoir en s'appuyant sur les ressources éducatives les plus concernées*"¹²⁰. Instauré en 2000, le Brevet informatique et internet (B2i), qui atteste le niveau acquis par les élèves des écoles, du collège, et prochainement du lycée dans la maîtrise des outils multimédias et de l'internet, reste largement centré sur la validation de compétences techniques plutôt qu'il n'éveille les jeunes internautes aux précautions qui doivent assortir certains usages du réseau. Le B2i n'est pas encore mis en œuvre dans tous les établissements scolaires concernés. Le Centre de Liaison de l'Enseignement et des Médias d'Information (CLEMI), un organisme de l'Education nationale, et l'Université belge de Louvain ont développé, avec le soutien de l'Union européenne, un *kit* de sensibilisation et d'éducation critique aux usages de l'internet à

¹¹⁶ Voir : <http://www.webaverti.ca/>

¹¹⁷ Voir : <http://www.getnetwise.org/>

¹¹⁸ Voir : <http://www.websafecrackerz.co.uk/>

¹¹⁹ LE FORUM DES DROITS SUR L'INTERNET, op. cit.

¹²⁰ Lettre de Xavier Darcos, ministre délégué à l'Enseignement scolaire, aux rectrices et recteurs d'académie. 26 janvier 2004 - <http://www.educnet.education.fr/chrgt/courrierRecteurs04.pdf>.

destination des éducateurs et des parents de qualité¹²¹. Cette initiative, toutefois, n'a pas encore été déployée à une large échelle auprès des établissements scolaires français.

De nombreuses expérimentations se sont développées, souvent isolément, au sein de certaines classes. Ces travaux sont suivis par différentes instances éducatives, en particulier les cellules TICE dépendant des recteurs d'académie et les centres régionaux et départementaux de documentation pédagogique. Des formations sont dispensées dans les académies et les départements aux enseignants du primaire et du secondaire, en formation continue comme dans les instituts universitaires de formation des maîtres (IUFM). Ces diverses expérimentations et initiatives pédagogiques sur les aspects civiques et éthiques de l'internet ne semblent toutefois faire l'objet que de d'une faible coordination.

Développée en partenariat avec plusieurs acteurs publics et privés, une récente initiative du ministère de l'Education nationale, de l'Enseignement supérieur et de la Recherche s'est donnée pour objectif de *"sensibiliser et informer les enfants, les parents et les enseignants des enjeux et des risques liés à l'utilisation de l'internet à l'école comme à la maison"* au cours de journées d'informations organisées dans toute la France à la demande d'établissements volontaires. Une première campagne de ce "Tour de France des collèges" doit être entreprise de décembre 2004 à juin 2005¹²².

Les initiatives existantes sont le plus souvent isolées.

Diverses initiatives de sensibilisation plus ponctuelles ont vu le jour en France, à l'initiative d'acteurs institutionnels ou privés. Un guide Internet et familles, élaboré en 1999 par l'Association des fournisseurs d'accès et de services internet (AFA), l'Union nationale des associations familiales (UNAF) et la Délégation interministérielle à la famille (DIF), constitue sans doute le premier véritable outil de sensibilisation et de responsabilisation des jeunes sur l'internet. En mai 2004, en application des recommandations émises en février 2004, le Forum des droits sur l'internet a pris l'initiative de la publication, en partenariat avec Bayard Presse, les ministères délégués à la Recherche et à la Famille, le fournisseur d'accès à l'internet Wanadoo et l'Union nationale des associations familiales (UNAF), de 400 000 exemplaires de deux guides pratiques illustrés à destination des adolescents et de leurs parents, suggérant notamment quelques conseils de prudence élémentaires. Ces guides sont également diffusés en libre téléchargement sur les sites des partenaires¹²³, et seront prochainement réédités. Le site DroitDuNet.fr, également édité par le Forum des droits sur l'internet, informe spécifiquement parents et enfants de leurs droits, mais aussi des règles de prudence qu'il leur est recommandé d'observer dans leurs usages du réseau¹²⁴. Le fournisseur d'accès à l'internet AOL a lancé en septembre 2003 un *"programme ludo-éducatif pour sensibiliser les plus jeunes à la sécurité sur Internet"* intitulé "Code du Web". Cette initiative s'appuie sur un mini-site comprenant des conseils¹²⁵, un quiz et un dessin animé à vocation pédagogique, et sur l'organisation d'interventions dans des magasins d'une sélection de villes. Le site Mineurs.fr, édité par la Délégation aux usages de l'internet (DUI), recense ces initiatives et s'efforce de leur donner quelque visibilité.

Atypique, enfin, est l'initiative d'un groupe de programmeurs bordelais qui a rendu publique, en 2004, la première version d'un logiciel capable de bloquer la communication par un jeune utilisateur de services de *chat* de données personnelles que ses parents ont préalablement définies. Sans prétendre empêcher de manière absolue le jeune utilisateur ne communique des informations personnelles sur l'internet, les variations possibles de la composition de chaque mot étant infiniment nombreuses, les concepteurs du logiciel

121 Voir : <http://www.educaunet.org/>.

122 Voir : <http://www.unclitdeclic.net/>.

123 Voir par exemple : <http://www.droitdunet.fr/guide/>.

124 Voir notamment : <http://www.droitdunet.fr/juniors/> et <http://www.droitdunet.fr/parents/>.

125 Voir : http://www.aol.fr/declic_securite/.

semblent considérer ce dernier comme un outil utile à attirer l'attention d'un jeune enfant sur les risques qu'il peut encourir en communiquant ces données à un inconnu. *LogProtect* est distribué gratuitement sous licence de logiciel libre, et pourrait être intégré à des solutions logicielles de contrôle parental¹²⁶.

De même qu'ils n'abordent pas spécifiquement ces problématiques sur le support internet, les pouvoirs publics n'ont pas encore entrepris de campagne grand public sur ces thèmes, comme on a pu l'observer, par exemple, à l'initiative du *Home Office* en Grande-Bretagne. La contribution de l'Etat à la sécurisation de la navigation des jeunes usagers de l'internet et à l'information des adultes sur les utilisations du réseau paraît ainsi comporter encore une large marge de progression.

d. La contribution des logiciels de contrôle parental.

En plus de bloquer l'affichage de certains contenus inappropriés aux enfants, certains logiciels de contrôle parental permettent aux parents d'interdire aux jeunes utilisateurs de communiquer avec des personnes inconnues sur l'internet. Certains outils permettent ainsi aux parents de bloquer l'accès à certains protocoles de communication, interdisant ainsi l'usage de certains logiciels (logiciel de courrier électronique, de communication instantanée...), ou encore les communications directes avec des correspondants non agréés en premier lieu par les parents.

Le logiciel *LogProtect*, dont la vocation paraît en premier lieu pédagogique, se présente comme un complément à de tels outils.

Les outils de contrôle parental, pour utile que puisse être leur contribution, ne peuvent toutefois palier l'insuffisance de l'information des adultes et les carences de l'effort de sensibilisation destiné aux enfants.

¹²⁶ Voir : <http://www.logprotect.net/>

III. RECOMMANDATIONS

L'internet est porteur de formidables opportunités pour les jeunes. Ces derniers comptent parmi les utilisateurs les plus actifs et les plus curieux du réseau. Cependant, des activités et des contenus susceptibles de constituer une menace, directe ou indirecte, pour eux prospèrent aussi dans cet environnement.

Les présentes recommandations ont pour objectif de contribuer à renforcer les moyens de lutter contre la diffusion et le recel de contenus pédo-pornographiques sur l'internet, et de prévenir les risques que des contacts établis sur l'internet puissent préparer une atteinte sexuelle, une agression sexuelle ou une tentative d'agression sexuelle, un viol ou une tentative de viol sur un mineur.

L'examen des données disponibles établit incontestablement que le réseau est employé au profit de l'échange d'un volume important d'images pédo-pornographiques. Il confirme également que des adultes sont susceptibles d'identifier, de contacter et de "piéger" des enfants en tirant avantage des possibilités de mise en contact offertes par les applications les plus populaires de l'internet. L'ampleur de la menace, toutefois, reste difficile à évaluer.

Le préalable à toute action efficace contre ces atteintes et risques d'atteintes graves à l'encontre de mineurs consiste à prendre la mesure précise de ces phénomènes. Beaucoup de travail reste à entreprendre dans ce domaine pour obtenir une image nette, susceptible de guider précisément l'action publique et d'inspirer de nouvelles initiatives aux acteurs de l'internet.

Il se dégage depuis plusieurs années, parmi les Etats comme parmi l'ensemble des acteurs de l'internet, un véritable consensus à agir contre ces phénomènes : pouvoirs publics, acteurs économiques, associations. Ces derniers confirment, dans ces recommandations, leur volonté de participer, chacun à la mesure de ses capacités d'action et de ses responsabilités.

Aucune solution n'est, à elle seule, de nature à faire cesser ces activités. On ne saurait en particulier s'en remettre simplement au renforcement des dispositifs pénaux et à l'action des seuls pouvoirs publics pour atteindre ces objectifs. Les recommandations proposent par conséquent à l'ensemble des acteurs de l'internet (pouvoirs publics, acteurs économiques, associations, parents) la mise en place d'une diversité d'actions visant à lutter contre ces délits ou à prévenir les actes qui les préparent sur l'internet.

Mieux connaître les usages et les risques

1. Etudier les comportements des jeunes utilisateurs de l'internet et la diversité des risques auxquels ils peuvent être exposés sur le réseau.

Les usages de l'internet par les jeunes Français ne sont pas précisément connus. Les premiers travaux consacrés par le Forum des droits sur l'internet à la protection des mineurs sur l'internet dressaient le constat du *"défaut ou [de] l'obsolescence d'études du mode d'accès des jeunes à l'internet en France, de leurs pratiques sur le réseau et des circonstances de leur exposition à des contenus préjudiciables"*. Le Forum recommandait

alors que "soit entreprise, à l'initiative des pouvoirs publics, une veille nationale des usages de l'internet par les jeunes et de leur exposition en ligne à des contenus tenus pour préjudiciables par la loi"¹²⁷. Cette lacune paraissait en effet constituer un frein à l'appréciation des éventuels risques des usages de l'internet par les jeunes, et à la définition de politiques et d'outils adaptés.

Ce constat et ces recommandations concernant l'exposition des mineurs à des contenus préjudiciables sur l'internet restent d'actualité. Il importe de souligner que le rôle de l'internet dans la préparation d'atteintes ou d'agressions sexuelles ou de viols sur des mineurs sont également méconnus en France.

A - Etudier les usages et les comportements des mineurs sur l'internet

Le Forum des droits sur l'internet recommande que les pouvoirs publics constituent un pôle de veille des usages de l'internet par les jeunes. Ce pôle pourrait avoir mandat de recenser les études existantes dans ce domaine auprès des centres de recherche et des acteurs économiques, d'impulser de nouvelles études quantitatives (accès au réseau, fréquence d'utilisation, principaux sites et services, par exemple) et qualitatives (études comportementales) auprès de partenaires publics et privés, et de prendre l'initiative de sondages réguliers. Il serait ainsi à même de contribuer à identifier l'opportunité d'action et les champs d'action prioritaires de la puissance publique, tout comme les canaux de communication à privilégier pour sensibiliser les mineurs à des usages maîtrisés de l'internet. **Le Forum recommande que cette veille se concentre tout particulièrement sur les nouveaux supports d'accès et les applications émergentes du réseau, comme les différents services interactifs accessibles depuis les téléphones mobiles.**

Les missions de la Délégation aux usages de l'internet (DUI) "*de proposer les mesures propres à généraliser l'accès à l'internet ainsi que la formation des familles, des enfants et du grand public aux usages des nouvelles technologies*" et de "*[répondre] aux demandes de conseil et d'expertise qui lui sont adressées par les administrations centrales, les services déconcentrés de l'Etat, les collectivités territoriales et les autres acteurs du développement de l'accès du grand public à la micro-informatique, à l'internet et au multimédia*"¹²⁸ paraissent prédisposer cette administration à piloter une telle mission.

B - Identifier et étudier les risques auxquels les jeunes utilisateurs de l'internet sont susceptibles d'être exposés sur les espaces publics du réseau

Le Forum des droits sur l'internet recommande que les pouvoirs publics entreprennent une veille de l'exposition des mineurs sur l'internet à des actes participant à la préparation d'atteintes, d'agressions sexuelles ou de viols, que ces actes fassent ou non l'objet d'une incrimination pénale : harcèlement, propositions de nature sexuelle non sollicitées sur les espaces de discussion, tentatives de rencontres non sollicitées et agressions suite à des contacts noués sur l'internet...

Plusieurs organismes et services, comme par exemple l'Observatoire national de l'enfance en danger (ONED) ou l'institution du Défenseur des Enfants, paraissent susceptibles d'entreprendre une telle veille¹²⁹. Le Forum des droits sur l'internet

¹²⁷ LE FORUM DES DROITS SUR L'INTERNET, op. cit.

¹²⁸ Décret n° 2003-1168 du 8 décembre 2003 portant création d'une délégation aux usages de l'internet paru au J.O. n° 284 du 9 décembre 2003.

¹²⁹ L'Observatoire national de l'enfance en danger (ONED) doit "*[contribuer] au recueil et à l'analyse des*

recommande que le ministère en charge des affaires familiales et de l'enfance détermine quelle institution est le mieux à même de porter cette mission.

2. Recueillir et exploiter les statistiques policières et judiciaires pour mieux connaître les phénomènes.

Un indicateur statistique comptabilisant, sur des bases unifiées, l'activité des services de police et de gendarmerie et des tribunaux en matière d'usages de l'internet aux fins d'échanger des contenus pédo-pornographiques ou de préparer des atteintes, agressions sexuelles et viols sur mineurs pourrait contribuer à alimenter et à orienter utilement l'action répressive et les initiatives de prévention dans ces domaines. Un tel indicateur n'existe pas.

Il conviendrait que chaque service d'enquête rapporte effectivement l'ensemble de ses activités dans le domaine de la protection des mineurs sur l'internet à une structure de référence chargée de coordonner les actions des services de police et de gendarmerie dans ce domaine spécifique de la cybercriminalité. La création d'indicateurs de référence communs aux services de police, de gendarmerie et de la justice serait utile à la collecte de ces informations.

Enfin, certaines infractions spécifiques décrivant l'échange des contenus pédo-pornographiques ou les atteintes et agressions sexuelles ou viols sur mineurs au moyen d'un réseau de communications électroniques n'interviennent souvent qu'à titre secondaire dans les procédures où elles sont mentionnées, et échappent à toute comptabilité. Il apparaît souhaitable qu'elles soient consignées anonymement et alimentent les statistiques judiciaires.

Le Forum des droits sur l'internet recommande que les ministères de la Justice, de l'Intérieur et de la Défense mettent en place une base de données statistiques recensant les faits de détention et de diffusion de contenus pédo-pornographiques sur l'internet et d'agression de mineurs suite à des contacts établis sur l'internet.

Cette base de données devra être constituée dans le respect des règles qui gouvernent la protection de la vie privée et des données personnelles relatives aux auteurs et aux victimes d'infractions, des outils communs permettant le partage de l'information.

Le Forum des droits sur l'internet recommande que le ministère en charge des affaires familiales et de l'enfance soit rendu destinataire des données statistiques décrivant l'activité des services judiciaires en matière d'usages de l'internet aux fins d'échanger des contenus pédo-pornographiques ou de préparer des atteintes, agressions sexuelles et viols sur mineurs.

3. Organiser un rendez-vous annuel des acteurs de la protection des mineurs sur l'internet

La diversité des parties engagées en faveur de la protection des mineurs sur l'internet,

données et des études concernant la maltraitance envers les mineurs, en provenance de l'Etat, des collectivités territoriales, des établissements publics, des fondations et des associations" (loi n° 2004-1 relative à l'accueil et à la protection de l'enfance, art. 9). L'institution du Défenseur des Enfants est "chargé[e] de défendre et de promouvoir les droits de l'enfant consacrés par la loi ou par un engagement international régulièrement ratifié ou approuvé" (loi n° 2000-196 du 6 mars 2000 instituant un Défenseur des enfant, art. 1).

l'évolution rapide des usages du réseau par les jeunes et celle des moyens de sécuriser ces usages justifient que s'intensifie le dialogue entre ces différents acteurs, qui le plus souvent ignorent l'étendue des compétences et des initiatives des autres parties.

Le Forum des droits sur l'internet recommande l'organisation d'un rendez-vous annuel au cours duquel les pouvoirs publics, le réseau des associations et les acteurs économiques seraient amenés à échanger leurs connaissances et à rapprocher leurs actions en matière de protection des mineurs sur l'internet.

Des acteurs étrangers, en particulier européens, pourraient être invités à rendre compte de leurs actions et à témoigner de leur expérience dans ce cadre. Un tel rendez-vous permettrait enfin de rendre compte de la mobilisation des différentes parties en faveur du renforcement de la protection des mineurs sur l'internet en France.

Cette réunion régulière pourrait être organisée à l'initiative du ministère en charge des affaires familiales et de l'enfance.

Sensibiliser les jeunes internautes et les adultes

4. Mettre en œuvre une vaste campagne de sensibilisation du grand public.

Depuis plusieurs années, tant au niveau national qu'europpéen, la protection de l'enfance et la prévention des risques associés aux usages de l'internet font l'objet de rapports et recommandations qui tous soulignent la nécessité des politiques de sensibilisation et d'information du grand public. De nombreuses actions de communication ont été menées par une diversité d'acteurs institutionnels et associatifs sans cependant parvenir à un niveau satisfaisant d'information des enfants et des parents.

D'après un sondage Eurobaromètre réalisé fin 2003, une majorité (55%) de parents de jeunes utilisateurs de l'internet déclaraient souhaiter être mieux informés sur les moyens de sécuriser les usages de l'internet, de préférence *via* les canaux traditionnels : à la télévision (43%), par courrier (43%) et, dans une moindre mesure, par les journaux (31%)¹³⁰.

On comprend à la lecture de ces statistiques que, s'ils ont été accueillis favorablement par les internautes qui en ont bénéficié, les efforts de sensibilisation à des usages maîtrisés de l'internet qui ont déjà vu le jour en France n'ont toutefois pas atteint l'objectif légitime de sensibilisation du très grand public.

Le Forum des droits sur l'internet recommande que les pouvoirs publics prennent l'initiative d'une large campagne pluri-médias de sensibilisation aux usages maîtrisés de l'internet, à l'adresse des parents et des jeunes utilisateurs de l'internet.

Une telle campagne de type publicitaire (spots télévisés, radiophoniques, affichage, presse) pourrait avoir pour objectifs de faciliter la compréhension des usages des technologies de l'information par les parents, de souligner leur responsabilité et de valoriser leur rôle dans l'accompagnement de ces usages auprès des jeunes utilisateurs de l'internet. Elle viserait également à doter les jeunes utilisateurs des réflexes leur permettant des usages maîtrisés de l'internet.

¹³⁰ EUROPEAN UNION OPINION RESEARCH GROUP (EEIG), "Illegal and harmful content on the Internet", Special Eurobarometer 203/Wave 60.2, Bruxelles, Commission Européenne, mars 2004 - Sondage réalisé interrogés en France entre novembre et décembre 2003.

5. Mobiliser tous les canaux publics au profit d'une information complète des jeunes internautes et de leurs parents.

Le Forum recommande que cette campagne publicitaire soit associée à la création de supports d'information spécifiques au service des jeunes utilisateurs de l'internet et de leurs parents (émissions télévisées ou radiophoniques, numéro vert, site web...).

Aucun site *web* d'information sur la maîtrise des usages de l'internet ne touche encore le très grand public. **Le Forum des droits sur l'internet recommande qu'un site *web de référence* soit constitué en "guichet unique" de l'information des jeunes utilisateurs de l'internet et des adultes sur l'ensemble des précautions à observer pour un usage maîtrisé de l'internet. Ce guichet devra de surcroît orienter ses visiteurs vers toutes les ressources utiles et autres initiatives de formation et d'information en ce domaine.** Pour remporter l'adhésion du très grand public, et atteindre des objectifs d'audience élevés, ce site devrait s'adresser spécifiquement à chaque cible (jeunes enfants, pré-adolescents, adolescents, parents, éducateurs...) en tenant compte de son niveau d'expertise, mobiliser des personnalités susceptibles de porter efficacement les principaux messages auprès de chacune de ces cibles, et proposer une diversité d'activités pédagogiques.

Les parents attendent de la télévision qu'elle les informe sur les moyens de sécuriser les usages de l'internet de leurs enfants. Ce canal de communication n'a pourtant encore jamais servi de support pour des informations de ce type. Il apparaît important, au regard des enjeux de la protection de l'enfance et de l'éducation sur l'internet, que soit réaffirmée la vocation éducative du secteur public de l'audiovisuel.

Le Forum des droits sur l'internet recommande l'organisation d'une table ronde réunissant les responsables du secteur public de l'audiovisuel sous l'égide du Conseil Supérieur de l'Audiovisuel, afin d'envisager les modalités de production et de diffusion d'émissions récurrentes consacrées à l'éducation aux médias et incluant notamment des informations sur la prévention de certains risques des usages de l'internet par les plus jeunes et sur les moyens d'y parer.

Le Forum recommande que les acteurs économiques et les associations représentant les utilisateurs du réseau comme les familles participent de manière concertée à l'élaboration de cette campagne de sensibilisation et d'information, et qu'ils soient sollicités pour en assurer le relais auprès du grand public et des familles. Il paraît particulièrement important que l'ensemble des acteurs soit partie prenante de la conception du site de référence, "guichet unique" de l'information des jeunes utilisateurs de l'internet et des adultes.

Le Forum des droits sur l'internet recommande qu'une action d'information spécifique soit entreprise à destination des associations incluant la protection de l'enfance dans leurs missions, qui leur rappellent notamment la marche à suivre et le cadre juridique à observer pour signaler aux autorités compétentes les contenus ou les comportements illicites qui leur sont parfois rapportés.

6. Pour une éducation à des usages maîtrisés de l'internet à l'école.

Renouvelant ses premières recommandations de mars 2004, **le Forum des droits sur**

l'internet recommande que les pouvoirs publics favorisent le développement auprès des établissements scolaires du premier et du second degré d'une véritable éducation à la civilité de l'internet à destination des élèves, notamment les plus jeunes, et renforcent les objectifs et les moyens des établissements scolaires en matière d'information et de sensibilisation à des usages maîtrisés de l'internet, en sorte que chaque élève soit informé *a minima* des règles de prudence à adopter à l'égard de ses correspondants en ligne. Le Brevet informatique et internet (B2i) devrait être effectivement déployé dans tous les établissements scolaires, conformément à l'objectif formulé par le ministre de l'Education nationale dès 2000. Le B2i pourrait être étendu en sorte de valider la maîtrise des règles de prudence et d'éthique élémentaires qui doivent gouverner la découverte de l'internet par les mineurs.

Cette démarche de formation scolaire à des usages maîtrisés de l'internet devra prendre en compte et, le cas échéant, se combiner aux autres initiatives de sensibilisation, d'information et de formation à destination des enfants et des familles entreprises à l'initiative de l'Etat et de la société civile.

7. Mobiliser les parents avec le soutien des associations familiales.

Il est essentiel que les parents de jeunes usagers de l'internet exercent pleinement leur responsabilité d'adultes au cours des premières années d'utilisation du réseau par leurs enfants.

Il paraît par exemple essentiel que les parents des jeunes internautes accompagnent ceux-ci dans leur découverte du réseau, qu'ils placent l'ordinateur familial dans une pièce commune plutôt que dans la chambre de l'enfant, et ne permettent l'utilisation de certains outils comme la *webcam* par leurs plus jeunes enfants qu'en leur présence. Il apparaît souhaitable que les parents entretiennent un dialogue suivi avec leurs enfants au sujet de leurs perceptions et de leurs expériences de l'internet.

Les parents de jeunes enfants pourront également choisir d'adopter un outil de contrôle parental permettant notamment de limiter les communications de leurs enfants les plus jeunes à une liste prédéterminée de correspondants. L'usage de tels outils ne saurait toutefois intervenir qu'en complément de la vigilance des parents. Aucun outil de contrôle parental n'est en effet infaillible, ni ne saurait suppléer le rôle éducatif des parents.

Le Forum des droits sur l'internet recommande que les associations familiales et de parents d'élèves prennent, en partenariat avec les pouvoirs publics, une part active à la sensibilisation des parents aux enjeux de la maîtrise des usages de l'internet et les assistent dans l'exercice de leur pleine responsabilité d'adultes sur l'internet. De telles initiatives pourront prolonger utilement d'autres campagnes de sensibilisation, d'information et de formation tournées vers les jeunes utilisateurs de l'internet.

8. Encourager fournisseurs d'accès et exploitants de services à adopter un standard élevé d'information des usagers de leurs services.

A en croire l'Eurobaromètre publié en mars 2004, les fournisseurs d'accès à l'internet et de services de télécommunication figurent en bonne place parmi les sources dont les parents de jeunes internautes attendent qu'ils les informent sur la maîtrise des usages de l'internet¹³¹.

¹³¹ 28% des parents de jeunes internautes indiquent attendre des informations sur les moyens de sécuriser les

De nombreux fournisseurs d'accès à l'internet (FAI) ont déjà entrepris, suite aux premiers travaux du Forum des droits sur l'internet relatifs à la protection de l'enfance, d'établir sur la page d'accueil de leurs sites un lien "Protection de l'enfance" menant vers une page d'information dédiée de leurs sites ou du site Pointdecontact.net, opéré par l'Association des fournisseurs d'accès et de services internet (AFA). Les fournisseurs d'hébergement et d'accès internet "grand public" membres de l'AFA se sont aussi engagés, dans la "Charte des prestataires de services d'hébergement en ligne et d'accès à Internet en matière de lutte contre certains contenus spécifiques" de juin 2004 "à rendre facilement accessibles depuis leurs portails, des informations (...) destinées à aider les parents à protéger leurs enfants sur Internet."

Le Forum des droits sur l'internet encourage l'ensemble de la profession à mettre en place un dispositif comparable à celui détaillé dans la charte des prestataires membres de l'AFA et à adopter un standard élevé d'information de leurs abonnés en matière de contrôle parental. Le Forum encourage notamment l'ensemble des prestataires de services à réserver sur leurs sites une bonne visibilité à un lien "Protection de l'enfance" renvoyant vers des contenus destinés à aider les parents à protéger leurs enfants sur l'internet.

Développer les outils favorisant la maîtrise des usages de l'internet

9. Renforcer les outils à la disposition des jeunes utilisateurs d'espaces interactifs et de logiciels de messagerie instantanée.

Les services interactifs et les applications de messagerie instantanée connaissent un succès grandissant parmi les jeunes utilisateurs de l'internet. Par leurs choix, les exploitants de ces services peuvent contribuer à limiter les risques que ces outils soient détournés de leur finalité par des adultes mal intentionnés à l'encontre de mineurs.

Par une charte signée le 14 juin 2004, les fournisseurs d'accès et d'hébergement "grand public" membres de l'Association des fournisseurs d'accès et de services internet (AFA) se sont engagés à établir des liens vers "un formulaire de signalement d'abus" permettant aux utilisateurs "de signaler directement au prestataire du service d'hébergement concerné, ou au Point de contact de la profession accessible à l'adresse www.pointdecontact.net, ou aux autorités publiques dûment habilitées, tout contenu en ligne visé par [ladite] charte", "sur tous les espaces communautaires, objets de leurs services d'hébergement - tels que les forums de discussion, "chats", salons -, sur les pages d'accueil de leurs services, et le cas échéant, sur les pages de listes de réponses des moteurs de recherche intégrés à leurs portails, de manière à ce que ces usagers puissent effectuer ce signalement d'un seul « clic »" (art. 2). **Le Forum des droits sur l'internet recommande que l'ensemble de la profession, exploitants de espaces communautaires ouverts au public (forums de discussion, chats, services de rencontres et communautaires ouverts aux adolescents) en particulier, se conforment aux bonnes pratiques que décrit cette charte.**

Certains exploitants de services interactifs et éditeurs de logiciels de

messagerie instantanée mettent en garde les jeunes internautes contre l'usage préjudiciable pouvant être fait du réseau par des personnes mal intentionnées, et leur adressent des conseils de prudence élémentaires. Le Forum des droits sur l'internet recommande que l'ensemble des exploitants de services et éditeurs de logiciels interactifs publient de telles mises en garde. Ces messages pourraient par exemple être mis en évidence dans les espaces interactifs dédiés aux mineurs ou portant sur des thématiques les concernant au premier chef lors, le cas échéant, du téléchargement de l'application, de l'ouverture d'un compte d'utilisateur ou d'un profil public accessible à tous les utilisateurs du service, voire à l'ouverture de chaque session, sous réserve de faisabilité technique. Ces exemples pourront être adaptés en fonction du service, dans le souci de permettre la réception optimale de l'information par le jeune public. L'étude spécifique des usages de ces applications et services par les jeunes utilisateurs de l'internet et la mesure régulière de l'efficacité de ces messages pourront contribuer à renforcer l'impact de ces initiatives.

Le Forum des droits sur l'internet recommande aux exploitants de services interactifs et aux éditeurs de logiciels de messagerie instantanée que les utilisateurs de leurs services bénéficient de fonctionnalités leur permettant de ne plus recevoir de messages d'un utilisateur en particulier et de bloquer la réception des messages d'utilisateurs ne figurant pas dans la liste de leurs contacts habituels, lorsque le service s'y prête.

Le Forum des droits sur l'internet recommande que soient explicitement affichées à l'entrée de tout espace interactif public son thème, le cas échéant la tranche d'âge à laquelle il s'adresse et la présence ou non de modérateurs.

Le Forum des droits sur l'internet recommande qu'il soit possible aux usagers de salons de discussion dédiés aux mineurs - ou portant sur des thématiques les concernant au premier chef - de contacter à tout moment un adulte référent, clairement identifié comme tel, compétent pour leur venir en aide et pour signaler, le cas échéant, un comportement préjudiciable aux mineurs aux autorités de police.

<p>10. Renforcer la maîtrise de la diffusion de données personnelles relatives à des mineurs sur l'internet.</p>

Les données personnelles de mineurs peuvent, lorsqu'elles sont rendues publiques, permettre à un adulte mal intentionné d'identifier de potentielles victimes, et parfois de les contacter directement et personnellement. Il paraît important, alors que les mineurs utilisent de plus en plus massivement l'internet et ses applications interactives, de renforcer la protection de leurs données personnelles.

A - Dans le cadre des services et applications interactifs de l'internet

Les services interactifs et plates-formes de discussion en ligne comme les *chats* ou les logiciels de messagerie instantanée exercent un fort attrait sur les jeunes utilisateurs de l'internet, qui peuvent y être contactés par d'autres utilisateurs mal intentionnés. De tels cas de figure peuvent également se présenter sur certains sites de rencontres et de services communautaires s'adressant spécifiquement aux mineurs.

Certains exploitants de services et éditeurs de ces logiciels conseillent à leurs jeunes utilisateurs, lors du choix de leur pseudonyme ou lorsqu'il leur est proposé de déclarer des informations nominatives (nom, prénom, âge ou date de naissance, ville, adresse,

numéro de téléphone, adresse de courrier électronique, par exemple), de ne pas rendre publiques d'informations les identifiant. **Le Forum des droits sur l'internet recommande que l'ensemble des exploitants de services interactifs et éditeurs de logiciels de messagerie instantanée adoptent cet usage** lorsque la nature et la finalité du service s'y prêtent.

Le Forum des droits sur l'internet recommande de plus que tout utilisateur puisse avoir le choix de ne pas publier d'informations nominatives non nécessaires au fonctionnement du ou des services. Un enfant devrait par exemple pouvoir rejoindre un salon de discussion ouvert au public sans toutefois devoir communiquer aux autres utilisateurs du *chat* de données personnelles comme son âge et sa ville de résidence.

B - Sur le web, en particulier dans le cadre des activités associatives ou scolaires

L'article 9 du Code civil dispose que "*chacun a droit au respect de sa vie privée*", et donne à toute personne un droit exclusif sur son image et sur l'utilisation qui en est faite, sauf intérêt légitime de tiers. L'autorisation de la personne représentée ou du titulaire de l'autorité parentale lorsque la personne est mineure et non émancipée, les mineurs ne disposant pas de leurs droits, est par conséquent indispensable.

Les articles 226-16 et suivants du Code pénal et la loi 78-17 du 6 janvier 1978 sur l'informatique et les libertés interdisent tout traitement informatisé de données personnelles lorsqu'il ne satisfaisait pas à certaines conditions. Il convient notamment par principe que la personne dont les données doivent faire l'objet d'une publication sur un réseau informatique comme l'internet consente à ce traitement. L'autorisation ne peut être délivrée que par le titulaire de l'autorité parentale si la personne est mineure et non émancipée.

Le Forum des droits sur l'internet rappelle les dispositions de la loi française aux éditeurs de sites personnels et associatifs (associations sportives, associations de parents d'élèves...), et leur recommande de ne pas publier sur leurs pages web la photographie ou les données personnelles d'un mineur sans l'accord explicite des titulaires de l'autorité parentale.

Le Forum des droits sur l'internet recommande que les établissements scolaires veillent tout particulièrement à respecter les termes de la loi en matière de diffusion de l'image ou des données personnelles de personnes mineures, et qu'ils évitent en règle générale de rendre publiques de telles informations sur leurs sites web.

11. Donner aux parents les moyens de choisir les meilleurs outils permettant de renforcer la sécurité des jeunes utilisateurs.

Les pouvoirs publics ont contribué au renouvellement, en mai 2004, de l'étude comparative des outils de contrôle parental réalisée par l'Institut National de la Consommation (INC). Compte tenu de l'évolution rapide des techniques de contrôle parental et de l'information encore lacunaire dont disposent les parents sur ces outils, le Forum des droits sur l'internet encourage les pouvoirs publics à conclure avec l'INC un accord pluriannuel permettant la mise à jour régulière de cette étude.

Le Forum recommande également que les prochaines éditions de cette étude

mettent spécifiquement en valeur les outils permettant de renforcer la sécurité des jeunes utilisateurs des applications interactives de l'internet (courrier électronique, messagerie instantanée, P2P...).

Engager une réflexion spécifique sur le droit et l'organisation du dispositif répressif

12. Approfondir la réflexion sur d'éventuelles évolutions du droit.

A - Mesurer les opportunités d'évolution du droit pénal

Le droit pénal français incrimine plusieurs comportements dont peut être victime un mineur : l'atteinte sexuelle "*sans contrainte, menace, ni surprise*", l'agression sexuelle ou le viol et leurs tentatives, qui supposent que l'acte délictueux soit consommé ou que soit constaté un commencement d'exécution. La chambre criminelle de la cour de cassation adopte une conception constante du commencement d'exécution qui doit associer une intention irrévocable et un lien de causalité suffisamment étroit et direct entre le comportement et l'infraction consommée ("*des actes qui tendent directement au crime avec intention de la commettre*", "*des actes qui tendent directement et immédiatement à la réalisation du délit*", ou encore "*des actes devant avoir pour conséquence directe et immédiate de consommer le crime, celui-ci étant ainsi entré dans la période d'exécution*"). L'internet peut servir à préparer ces infractions, la mise en relation d'adultes déterminés à commettre une atteinte ou une agression sexuelle à l'encontre de mineurs étant notamment possible sur les espaces interactifs de communication électronique comme en d'autres lieux.

Il n'existe pas, en droit français, d'infraction décrivant spécifiquement le fait, pour un adulte, de rechercher les faveurs sexuelles de mineurs, en ligne ou hors ligne, ou le fait de rencontrer un mineur dans l'intention de commettre une atteinte ou une agression sexuelle ou un viol. Certains membres des forces de police et associations de protection des droits des enfants déplorent cette situation, et souhaitent la création d'une infraction pénale spécifique au fait, pour un adulte, de rechercher sur l'internet les faveurs sexuelles d'un mineur. Ces acteurs considèrent qu'une telle incrimination nouvelle serait seule capable de permettre la répression de certaines prises de contact avant que ne soit effective une agression physique, et de renforcer les moyens de dissuader des adultes mal intentionnés d'entreprendre de telles démarches. Si l'on conçoit aisément l'intérêt d'un tel dispositif en termes, notamment, de dissuasion, ce dernier n'en paraît pas moins contraire aux principes de droit pénal qui excluent que l'on puisse incriminer une simple intention.

Le Forum des droits sur l'internet recommande aux ministères de la Justice et de l'Intérieur d'examiner et de provoquer un débat sur l'opportunité de créer ou non une nouvelle incrimination pénale punissant le fait, pour un adulte, d'émettre des propositions à caractère sexuel à destination de mineurs, ou de chercher à rencontrer un mineur auquel il aurait adressé des propositions à caractère sexuel.

B - Envisager l'évolution des moyens de la procédure pénale

Les faits de détention, de recel ou de diffusion de pédo-pornographie ne figurent pas au nombre des infractions citées par l'article 706-73 du Code de procédure pénale, qui établit la liste des incriminations auxquelles sont applicables les procédures spéciales décrites par la loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité. Ces procédures particulières, relatives notamment à l'infiltration (art. 706-81 du CPP), aux perquisitions (art. 706-89 et suivants du CPP) et à l'interception de correspondances émises par la voie des communications (art. 706-96 du CPP), ne sont donc pas applicables aux enquêtes sur les échanges en ligne d'images pédo-pornographiques. Le Garde des Sceaux avait pourtant indiqué à plusieurs reprises, au cours des débats parlementaires qui ont préparé le vote de la loi, que *"la criminalité organisée (...), ce sont les enlèvements, les trafics de stupéfiants, le terrorisme, la traite des êtres humains, les meurtres en bande organisée, les braquages en bande organisée, le proxénétisme aggravé, la pédo-pornographie par Internet"*¹³².

Certains représentants des autorités répressives souhaitent que les procédures spéciales prévues par la loi du 9 mars 2004 soient élargies à la recherche des auteurs de faits de diffusion d'images pédo-pornographiques, permettant ainsi aux enquêteurs de recourir, dans un cadre proprement défini par la loi, à l'emploi d'identités d'emprunt ou fictives, et de procéder légitimement à la recherche proactive de contenus illicites, à l'exclusion de toute démarche de provocation. Cette évolution maîtrisée des moyens procéduraux des services de police permettrait également d'encadrer l'utilisation par les enquêteurs de moyens de paiement, lorsqu'ils sont requis à l'entrée d'un site ou d'un service en ligne, pour vérifier une infraction.

L'élargissement des moyens de procédure prévus par la loi du 9 mars 2004 ne peut toutefois être envisagé sans étude spécifique des conséquences de l'extension éventuelle de ces moyens à la recherche des auteurs de faits de diffusion d'images pédo-pornographiques, particulièrement en matière de sauvegarde des libertés publiques. Un dispositif alternatif à l'extension des moyens de procédures prévus par la loi du 9 mars 2004 pourrait ainsi être imaginé pour répondre aux principales demandes des enquêteurs.

Le Forum recommande également aux pouvoirs publics d'examiner l'opportunité d'élargir certaines des dispositions de la loi du 9 mars 2004, comme l'infiltration, aux enquêtes portant sur la diffusion de matériels pédo-pornographiques sur l'internet. Les pouvoirs publics pourraient également choisir de privilégier un dispositif alternatif permettant aux agents des forces de l'ordre de rechercher ces infractions sous le couvert d'une identité d'emprunt ou fictive, et de les constater sur des serveurs auxquels l'accès est conditionné par l'utilisation d'un moyen de paiement. Ces opérations devraient être réalisées sous le contrôle de l'autorité judiciaire.

13. Adapter l'organisation des services d'enquête.

Les services d'enquête prenant part à la lutte contre la pédo-pornographie sur l'internet se sont pour l'essentiel organisés au gré des compétences et des initiatives de certains enquêteurs. L'efficacité de cette lutte paraît souffrir de la dispersion de l'information utile aux enquêtes et du manque de coordination entre services.

¹³² Dominique Perben, Garde des Sceaux. Assemblée nationale, Troisième séance du jeudi 5 février 2004 - 154e séance de la session ordinaire 2003-2004 - <http://www.assemblee-nat.fr/12/cr/2003-2004/20040154.asp>.

Le Forum des droits sur l'internet approuve le projet présenté le 7 septembre 2004 par le ministre de l'Intérieur, de la sécurité intérieure et des libertés locales de faire de certains services d'enquête des référents nationaux pour certaines infractions commises par le biais de l'internet et des réseaux.

Le Forum recommande que le pôle de compétence chargé de la veille des contenus pédo-pornographiques sur l'internet dispose des moyens nécessaires à l'exercice de sa mission, et agisse en total synergie avec les autres services concernés de l'Etat.

Le Forum des droits sur l'internet recommande que ce pôle soit conçu comme un outil de mutualisation des informations relatives à toutes les enquêtes en matière de pédo-pornographie sur l'internet, rassemblant et favorisant le partage et le recoupement de ces informations entre tous les services concernés au niveaux national et international.

Le Centre national d'analyse des images pédo-pornographiques (CNAIP), qui centralise les images saisies dans le cadre des enquêtes de police et de gendarmerie et met le produit de leur analyse à la disposition des services d'enquête, fonctionne déjà selon ce principe.

En revanche, un tel pôle de veille ne saurait toutefois se substituer aux services d'enquête. Ses pratiques se conformeraient naturellement aux règles qui régissent la protection des données à caractère personnel.

Le Forum des droits sur l'internet recommande que le pôle de veille établisse et remette aux ministres concernés un rapport d'activité annuel faisant notamment état de la coopération entre les services.

14. Former enquêteurs et magistrats aux techniques et aux procédures de la recherche d'infractions sur l'internet et les supports informatiques.

Le Forum des droits sur l'internet approuve résolument le projet annoncé en septembre 2004 par le ministre de l'Intérieur, de la sécurité intérieure et des libertés locales d'accélérer l'effort de formation des enquêteurs spécialisés au sein de la police et de la gendarmerie et d'en porter le nombre à 700 à l'horizon 2007.

Le Forum recommande également que des magistrats référents en matière de cybercriminalité soient spécifiquement formés et renforcent les ressources des parquets généraux et des chambres d'instruction de chaque ressort de cour d'appel.

15. Clarifier le dispositif encadrant la conservation des données de connexion.

Les autorités de police et de gendarmerie sont fréquemment amenées à requérir la transmission d'informations permettant l'identification d'utilisateurs du réseau auprès des opérateurs et exploitants de services de la société de l'information. Les décrets d'application de l'article L.34-1 du code des postes et des communications électroniques et des dispositions de l'article 6-II de la loi du 21 juin 2004 pour la confiance dans

l'économie numérique doivent encore préciser la nature et la durée de stockage des données de connexion à conserver par les opérateurs techniques. Ces décrets doivent aussi éclaircir les modalités d'exécution des réquisitions judiciaires.

Le Forum des droits sur l'internet recommande que les pouvoirs publics fixent rapidement le cadre réglementaire relatif à la conservation des données de connexion, satisfaisant aux impératifs des forces de sécurité comme aux contraintes des opérateurs et exploitants de services, dans le respect des libertés publiques.

Renforcer la coopération internationale policière et judiciaire

La coopération et l'entraide internationale sont l'un des dispositifs fondamentaux d'une lutte efficace contre la diffusion de contenus illicites sur l'internet, et tout particulièrement de pédo-pornographie. De nombreux dispositifs internationaux pertinents restent toutefois inappliqués.

16. Mettre en œuvre et promouvoir les dispositions de la Convention sur la cybercriminalité en matière de lutte contre la pédo-pornographie.

La Convention sur la cybercriminalité du Conseil de l'Europe peut constituer une avancée considérable en matière d'unification de la politique de lutte contre la diffusion de matériels pédo-pornographiques des Etats qui y adhèrent, et un outil de coopération policière et judiciaire prometteur. **Le Forum des droits sur l'internet recommande que la France ratifie et adopte au plus tôt les dispositions de la Convention sur la cybercriminalité relatives à la lutte contre la diffusion de contenus pédo-pornographiques sur l'internet.**

Le Forum des droits sur l'internet recommande que la France encourage certains Etats membres ou associés du Conseil de l'Europe, en particulier la Fédération de Russie, à signer et ratifier la Convention sur la cybercriminalité. Le Forum des droits sur l'internet recommande également que la France conclue, avec les principaux Etats non signataires de la Convention sur la cybercriminalité, des conventions bilatérales de coopération policière et d'entraide judiciaire en matière pénale renforçant les moyens de la lutte contre la cybercriminalité.

Le Forum recommande que les ministères concernés préparent un bilan national de la coopération d'entraide judiciaire et policière entre les Etats, concernant notamment les mesures préconisées par la Convention sur la cybercriminalité, afin d'en évaluer l'efficacité et, le cas échéant, de proposer des aménagements du texte au Conseil de l'Europe.

17. Renforcer la coopération, l'entraide judiciaire et les échanges de bonnes pratiques au sein de l'Union européenne.

Le Forum des droits sur l'internet recommande que s'intensifient la coopération policière, l'entraide judiciaire et les échanges de bonnes pratiques au niveau européen.

La Convention d'entraide de l'Union européenne promet la simplification et l'accélération

des demandes d'entraide judiciaire entre Etats membres, de magistrat à magistrat, et conformément aux procédures et aux formalités ayant cours dans l'Etat requérant. **Le Forum des droits sur l'internet recommande que la France ratifie au plus tôt la Convention d'entraide judiciaire de l'Union européenne.**

Le Forum des droits sur l'internet recommande également que les pouvoirs publics français favorisent l'organisation de rencontres informelles entre les autorités nationales et certains de leurs homologues européens, qui pourront les faire bénéficier de leur expérience et de leurs bonnes pratiques en matière de lutte contre la pédo-pornographie et la pédophilie sur l'internet.

CONCLUSION : POURSUIVRE LA REFLEXION SUR LES RESEAUX MOBILES ET LES NOUVEAUX SUPPORTS D'ACCES A L'INTERNET

Les présentes recommandations dessinent un ensemble de pistes d'action tendant à renforcer les moyens de lutter contre la représentation et la préparation, sur l'internet, d'atteintes sexuelles à l'encontre de mineurs. Elles réaffirment la détermination des acteurs français de l'internet à défendre l'avenir des "Enfants du Net", et ont pour vocation d'inspirer l'action de l'ensemble des acteurs, et tout particulièrement des pouvoirs publics.

Les responsables politiques se sont désormais associés à cette réflexion : le ministre des Solidarités, de la Santé et de la Famille a annoncé en décembre 2004 que "*la sécurisation des usages de l'Internet par les mineurs afin de participer à la lutte contre la pédopornographie*" ferait l'objet de l'un des groupes de travail de la conférence de la famille 2005 ; le ministre de l'Intérieur, de la Sécurité intérieure et des Libertés locales a annoncé, en septembre 2004, sa décision de renforcer spécifiquement les moyens des services de police et de gendarmerie en matière de cybercriminalité ; le ministre de la Jeunesse, de l'Education nationale et de la Recherche avait dévoilé, en janvier 2004, son plan pour la sécurisation des usages de l'internet à l'école. Lors d'une conférence organisée à Bruxelles en novembre 2004, l'association belge Child Focus a su attirer l'attention des "First Ladies" de grands pays d'Europe et de nombreux décideurs européens sur certains usages de l'internet potentiellement particulièrement préjudiciables aux mineurs.

*

Ces recommandations traitent des usages de l'internet accessibles depuis les terminaux d'accès à l'internet les plus communs que sont les micro-ordinateurs. Ces applications ne doivent pas occulter les prochains usages de l'internet et les promesses des nouveaux supports d'accès au réseau.

Les dernières générations de réseaux et de téléphones mobiles sont en particulier devenus de véritables plates-formes multimédias donnant accès à de nombreux usages interactifs : courrier électronique, *chat*, enregistrement et diffusion d'images fixes ou animées, visioconférence, partage de fichiers, par exemple.

A ces nouveaux usages peuvent correspondre de nouveaux mésusages qu'il conviendra de prendre en compte dans l'intérêt de la protection des mineurs, d'autant plus que ces derniers sont nombreux à posséder un téléphone mobile¹³³, et parmi les premiers à en explorer les nouveaux usages.

Les opérateurs de téléphonie mobile français sont sensibles à ces enjeux et souhaitent engager une réflexion sur les moyens spécifiques à mettre en œuvre pour renforcer la protection des mineurs dans le cadre de l'utilisation d'applications multimédias mobiles.

Le Forum des droits sur l'internet encourage cette démarche et recommande que de prochains travaux étudient les réponses spécifiques aux applications et aux supports mobiles qui pourraient être apportées en matière de protection des mineurs.

¹³³ Selon le CREDOC, 63% des 12-17 ans étaient équipés d'un téléphone mobile en juin 2003 (Régis BIGOT, op. cit.), ainsi que 5 % des 7-10 ans interrogés dans le cadre d'une étude TNS) 5 % des 7-10 ans interrogés dans le cadre d'une étude TNS (TNS-SOFRES, juin 2004).

Annexes

Annexe 1 : Composition du groupe de travail

Odile AMBRY

Vice-présidente
Internet Society (ISOC), Chapitre français

Patrice BLANC

Secrétaire général
Institution du Défenseur des Enfants

Martine BROUSSE

Présidente
La Voix de l'Enfant

Philippe CAILLOL

Chef du bureau du régime juridique de la presse et des services d'information
Direction du développement des médias (DDM) - Premier ministre

Coralie CAPILLON

Juriste
La Voix de l'Enfant

Estelle DE MARCO

Juriste
Association des Fournisseurs d'Accès et de Services Internet (AFA)

Isabelle FALQUE-PIERROTIN

Déléguée générale
Le Forum des droits sur l'internet

Joël FERRY

Officier de gendarmerie
Ministère de la Justice
Direction des Affaires Criminelles et des Grâces (DACG)

Axelle HOVINE

Adjointe au chef du bureau du régime juridique de la presse et des services d'information
Direction du développement des médias (DDM) - Premier ministre

Guillaume LE FRIANT

Lead Programming Manager
MSN France

Jean-Paul LEROUX

Responsable concurrence et déontologie
Orange France

Stéphane MARCOVITCH

Délégué général
Association des Fournisseurs d'Accès et de Services Internet (AFA)

Olivier PERALDI

Adjoint au délégué
Délégation interministérielle à la Famille (DIF)

Myriam QUEMENER

Magistrate - Chef du bureau des Politiques Pénales Générales et de la Protection des Libertés Individuelles
Direction des Affaires Criminelles et des Grâces (DACG)
Ministère de la Justice

Jean-Pierre QUIGNAUX

Chargé de mission
Union Nationale des Associations Familiales (UNAF)

Anne TERRIER

Chargée de mission
Institution du Défenseur des Enfants

Rapporteur du groupe de travail :

Matthieu LERONDEAU

Chargé de mission
Le Forum des droits sur l'internet

Annexe 2 : Auditions et entretiens entrepris par le groupe de travail

Chantal D'ABOVILLE (entretien)

Administratrice
Innocence en Danger

Alain BOULAY

Président
Association d'aide aux parents d'enfants victimes (APEV)

Catherine CHAMBON

Commissaire divisionnaire
Office central de lutte contre la criminalité liée aux technologies de l'information (OCLCTIC)

Sylvie CLEYET

Responsable du projet Assurnet contre la cyberpedocriminalité
Région Rhône-Alpes

Marcel FAURE

Commissaire divisionnaire
Division nationale pour la répression des atteintes aux biens et personnes (DNRAPB)

Divina FRAU-MEIGS

Professeur de sociologie des médias
Universités d'Orléans et Paris I Panthéon-Sorbonne

Eric FREYSSINET (entretien)

Chef d'escadron de gendarmerie
Chef du département INL
Institut de recherche criminelle de la gendarmerie nationale (IRCGN)

Fabrice GAUTHIER

Commandant de police
Brigade de protection des mineurs (BPM) de Paris

Arnaud GRUSELLE

Président
Fondation pour l'enfance

Philippe JARLOV

Adjudant-chef de gendarmerie
Section des Recherches de Bordeaux

Philippe JEAMMET

Professeur de psychiatrie
Institut Mutualiste Montsouris (IMM), Université Paris-V René Descartes
Président
Ecole des Parents et des Educateurs (EPE)

Marie LAJUS

Commissaire de police
Brigade de protection des mineurs (BPM) de Paris

Yvon TALLEC

Premier substitut du procureur – Chef du parquet des mineurs
Tribunal de grande instance (TGI) de Paris

Bernard VALADON

Président
Le Bouclier

Grégory VERET

Action Innocence Group (AIG)

Bibliographie

1. Ouvrages et rapports

John CARR. *Child abuse, child pornography and the Internet*. NCH, 2004.

CONSEIL DE L'EUROPE. *L'impact de l'utilisation des nouvelles technologies de l'information sur la traite des êtres humains aux fins d'exploitation sexuelle. Rapport final du groupe de spécialistes EG-S-NT*. Conseil de l'Europe (Direction générale des droits de l'homme, Division égalité entre les femmes et les hommes), septembre 2003.

LE FORUM DES DROITS SUR L'INTERNET. *Les Enfants du Net - (1) Les mineurs et les contenus préjudiciables sur l'internet*. Le Forum des droits sur l'internet, 2004.
<http://www.foruminternet.org/recommandations/lire.phtml?id=694>

HOME OFFICE TASK FORCE ON CHILD PROTECTION ON THE INTERNET. *Good practice models and guidance for the internet industry on: chat services, instant messaging (IM), web based services*. Home Office Communication Directorate, janvier 2003.
http://www.homeoffice.gov.uk/docs/ho_model.pdf

INTERNET WATCH FOUNDATION. *Annual Report 2003*. Internet Watch Foundation, 2003.

Kenneth V. LANNING. *Child Molesters: A Behavioral Analysis*. National Center for Missing & Exploited Children, National Center for Missing & Exploited Children (NCMEC), U.S. Department of Justice (Office of Juvenile Justice and Delinquency Prevention), septembre 2001.
http://www.missingkids.org/en_US/publications/NC70.pdf.

Agathe LEPAGE. *Libertés et droits fondamentaux à l'épreuve de l'internet*. Editions du Juris-Classeur, 2002.

Sheridan MORRIS. *The future of netcrime now*. Online Report 62/04. Home Office, Décembre 2004.

Part 1 – threats and challenges

<http://www.homeoffice.gov.uk/rds/pdfs04/rdsolr6204.pdf>

Part 2 – responses

<http://www.homeoffice.gov.uk/rds/pdfs04/rdsolr6304.pdf>

SENAT (Service des affaires européennes). "La lutte contre la pornographie enfantine". *Les documents de travail du Sénat. Série Législation comparée*, mai 2001, n°90.
<http://www.senat.fr/lc/lc90/lc90.html>

Alex TURK. *Quand les policiers succèdent aux diplomates*. Rapport d'information 523 (97-98). Sénat, 25 juin 1998.
<http://www.senat.fr/rap/r97-523/r97-523.html>

UNITED STATES GENERAL ACCOUNTING OFFICE. *File-Sharing Programs. Peer-to-Peer Networks Provide Ready Access to Child Pornography*. Report to the Chairman and Ranking Minority Member, GAO-03-351. House of Representatives (Committee on Government Reform), février 2003.
<http://www.gao.gov/cgi-bin/getrept?GAO-03-351>

Janis WOLAK, Kimberly MITCHELL, David FINKELHOR. *Internet Sex Crimes Against Minors: The Response of Law Enforcement*. National Center for Missing & Exploited Children (NCMEC), U.S. Department of Justice (Office of Juvenile Justice and Delinquency Prevention), novembre 2003.

http://www.missingkids.org/en_US/publications/NC132.pdf

2. Articles

Frédéric BARILLE. "Le pédophile chassait sur Internet". *Ouest-France*, 24 novembre 2004.

<http://www.brest.maville.com/actu/detail.asp?idDoc=181602&IdCla=19>

Martin BRIGHT. "BT puts block on child porn sites". *The Observer*, 6 juin 2004.

http://observer.guardian.co.uk/uk_news/story/0,6903,1232422,00.html

Roger DARLINGTON. "Sex on the Net", version du 2 août 2004.

<http://www.rogerdarlington.co.uk/sexonnet.html>

Arnaud DEVILLARD. "MSN ferme ses salons pour cause de dérive pornographique". *01Net*, 24 septembre 2003.

<http://www.01net.com/article/217608.html>

Jacky DURAND. "Villepin pour une lutte Net et sans bavure". *Libération*, 8 septembre 2004.

<http://www.liberation.fr/page.php?Article=237065>

Estelle DUMOUT, Jérôme THOREL. "LCEN: le Conseil constitutionnel censure l'«amendement Devedjian»". *ZDNet France*, 15 juin 2004.

<http://www.zdnet.fr/actualites/internet/0,39020774,39157007,00.htm>

Will GARDNER. "The Sexual Offences Bill: Progress and the Future". Discours prononcé lors de la conférence "Tackling Sexual Grooming", Londres, 29 septembre 2003.

<http://www.childnet-int.org/downloads/online-grooming2.pdf>

Margaret A. HEALY. "Child pornography: an international perspective". Document de travail. Congrès mondial contre l'exploitation sexuelle commerciale des enfants, Stockholm, 27-31 août 1996.

http://www.usemb.se/children/csec/child_pornography.html

Robert JACQUES. "Blair backs BT child porn prevention filter". *VNUNet.com*, 22 juillet 2004.

<http://www.vnunet.com/news/1156795>

Isabelle DE SCHRIJVER, Tom VAN RENTERGHEM, Heidi DE PAUW. "Child Pornography on the Internet". Présentation lors de la conférence "The Challenge of Cybercrime" (Conseil de l'Europe), Strasbourg, 15-17 septembre 2004.

http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Combating_economic_crime/Cybercrime/International_conference/Child%20Pornography%20on%20the%20Internet.pdf

"Online child safety drive launched". *BBC News - World Edition*, 6 janvier 2003.

http://news.bbc.co.uk/2/hi/uk_news/2629611.stm

"Cyber-cops to patrol Internet chatrooms". *CNN*, 9 juin 2004.

<http://www.cnn.com/2004/TECH/internet/06/09/crime.internet.reut/>

3. Enquêtes et sondages

David FINKELHOR, Kimberly MITCHELL, Janis WOLAK. *Online Victimization: A Report on the Nation's Youth*. National Center for Missing & Exploited Children (NCMEC), U.S. Department of Justice (Office of Juvenile Justice and Delinquency Prevention), juin 2000.
http://www.missingkids.org/en_US/publications/NC62.pdf

David FINKELHOR, Kimberly MITCHELL, Janis WOLAK. "Highlights of the Youth Internet Safety Survey". *OJJDP Fact Sheet*, mars 2001, n°4.
http://www.missingkids.org/en_US/documents/internetsafety_surv.pdf

Sonia LIVINGSTONE, Magdalena BOBER. *UK Children Go Online. Surveying the experiences of young people and their parents*. Economic & Social Research Council (ESRC), Juillet 2004.
<http://www.children-go-online.net/>

Céline METTON. "Ils s'aiment par Internet". *Informations sociales*, novembre 2003, n°111, pp. 32-41.

EUROPEAN UNION OPINION RESEARCH GROUP (EEIG). "Illegal and harmful content on the Internet". Special Eurobarometer 203/Wave 60.2, mars 2004.
http://europa.eu.int/information_society/programmes/iap/docs/pdf/reports/eurobarometer_survey.pdf

RESEAU EDUCATION-MEDIAS. *Young Canadians in a Wired World. Phase II. Focus Groups*. Réseau Education-Médias, février 2004.
http://www.media-awareness.ca/english/special_initiatives/surveys/index.cfm