# Pornographie, pédopornographique et violences sur internet
# Guide pratique en 8 points
# à l'usage des parents et de leurs enfants

Paul Guermonprez - paul@guermonprez.eu

10 avril 2009

# Table des matières

**Résumé**

La navigation sur internet comporte différents risques pour des enfants ou des adolescents. Certains sont théoriques d'autres réels, mais le doute alimente une psychose peu productive et potentiellement dangereuse. Ces dangers sont en fait la transcription sur internet de dangers existant dans la vie réelle, les auteurs et victimes sont les mêmes dans les deux cas. Le bon sens s'applique de la même manière mais nécessite de comprendre certaines différences d'ordre technique.

Voici une liste non exhaustive de huit risques pour les enfants ou adolescents, à replacer dans le contexte de votre famille et de vos méthodes éducatives. Ils sont accompagnés de solutions pratiques, de propositions de règles, mais aussi d'avertissements sur les fausses protections.

Ce document se réfère à des législations et jurisprudences de différents pays, il n'a pas pour objectif d'être précis du point de la loi Française. Il traite a la fois de pédopornographie et de pornographie, bien que les contenus et leur distribution soient totalement différents, parce qu'ils sont souvent victimes d'amalgame.

D'une manière plus générale voici trois règles de sécurité informatique qui sont applicables à la sécurité des personnes sur internet :

1. On est souvent trop paranoïaque avec les autres, et pas assez avec soi même.
2. Se croire protégé par une mesure technique préventive est un leurre qui peut vous mettre en danger.
3. La solution est souvent : éducation, audit, éducation, audit ...

# Chapitre 1

# Définitions

## Pornographie adulte

Produite par des adultes, destinée à des adultes, représentant des adultes.
La pornographie adulte est légale à produire et à regarder pour des majeurs (ou 12, 16 ans selon les contenus).

## Pornographie enfantine

Produite par des adultes pour d'autres adultes (pédophiles), avec des mineurs représentes (en général enfants impubères).
Illégal à produire, illégal à posséder ou consulter. Ceci vaut aussi pour des dessins, bandes dessinées ou des avatars en 3D.

## Pornographie des mineurs

Par des mineurs pour des mineurs. En pratique échange consentant en privé de photos au sein d'un couple d'adolescents âgés.
La loi est protectrice par défaut, elle englobe ces cas dans la pédopornographie et laisser au juge le soin de faire le tri en fonction du contexte.

## Pédophile

En psychiatrie, un pédophile est une personne adulte éprouvant une attirance sexuelle envers les personnes impubères.
Légalement, ce n'est pas le fait d'être pédophile qui est condamné, mais le fait de passer à l'acte (abus sexuel sur mineur ou pédopornographie). Dans le cadre juridique Français le concept inclus tous les mineurs et pas seulement les enfants impubères.

# Chapitre 2

# Danger physique

## 2.1 Rencontrer un pédophile

### Danger :

Entrer en contact avec un pédophile inconnu qui se poursuit par une rencontre dans la vie réelle (souhaitée ou pas, prévue ou pas).

### Spécificité d'internet :

Sur internet comme dans la vie réelle, il est facile de se construire une fausse identité et de mentir sur ses intentions. La spécificité d'internet pour les pédophiles est de pouvoir s'inventer plus facilement un faux âge, la faible prise de risque, la multiplication des tentatives de prise de contact et la possibilité de trouver des informations sur sa cible.
Réciproquement, un mineur pourra facilement prendre l'identité d'un majeur, par exemple sur un site de rencontre pour adultes (dans l'intention de jouer ou pas).

### Règles absolues :

1. Première règle absolue : Ne pas accepter les contacts avec des inconnus sur vos réseaux sociaux, chat, blogs. N'acceptez que les personnes que vous connaissez dans la vie réelle, n'acceptez pas les amis des amis si vous ne les connaissez pas personnellement. Cette règle est l'équivalent virtuel de "ne pas parler à des inconnus dans la rue". Au lieu d'utiliser internet pour provoquer de nouveaux contacts en grand nombre, utilisez le pour renforcer les contacts existants dans la vie réelle.
2. Seconde règle absolue : Ne pas donner son nom, adresse, des informations en général à un inconnu. Internet permet de remonter facilement votre piste et de peut être connaître votre nom, adresse, photo ... et aider à la rencontre réelle. Ne surtout pas jouer avec cette règle en se croyant protégé par l'anonymat supposé d'internet (il ne l'est pas tant que ça). Si vous avez suivi la première règle vous ne devriez pas être en contact avec des inconnus ... donc ne pas avoir à donner ce genre d'informations.
3. Troisième règle absolue : Refuser toute rencontre avec une personne que vous ne connaissez que par internet. Même si cette rencontre est anonyme, le sujet est innocent, dans un lieu public, même si vous discutez depuis 6 mois avec la personne, ne rencontrer sous aucun prétexte. Internet a cette particularité de pouvoir créer un sentiment de proximité et de confiance entre des individus qui ne se sont jamais rencontrés et ne se connaissent pas réellement. Il ne faut aussi pas dire ou vous vous trouverez à un moment donné, ce qui permettrait une rencontre.

4. Quatrième règle absolue : Ne jamais prendre l'identité d'un majeur lorsqu'on est mineur, même pour jouer, même en se croyant protégé par l'anonymat. L'anonymat comme une fausse identité n'est pas une protection car ils sont durs à maintenir.

### Parents :

A part leur apprendre et répéter les règles souvent, il peut être utile pour les plus petits de regarder de temps en temps en sa compagnie la liste des amis sur son système de communication et de se demander qui ils sont en pratique. Il est aussi utile de regarder (ou demander à votre enfant de vous montrer) son profil ou blog et vérifier qu'il ne contient aucune information permettant la localisation, l'identification ou le contact par email/chat par des inconnus. Son adresse email ne doit pas contenir le nom de famille, voire le prénom, un pseudo impersonnel est préférable. Dans la même optique, la photo de profil ou avatar peut aussi être remplacée par une photo déguisée ou un dessin, aussi personnalisée mais moins identifiable.

### Technique :

Le moyen principal de communication des jeunes sur internet est le "chat", ou dialogue écrit. Ces systèmes fonctionnent avec une liste de contacts. Un enfant peut avoir accès à de multiple systèmes selon le contexte, sur différents sites ou dans différents jeux connectés à internet.

1. Ajout de contacts : Il existe des systèmes de chat "verrouillés" pour jeunes enfants qui n'acceptent que les contacts que vous ajoutez positivement en tant que parent. Mais rapidement vous n'éviterez pas votre enfant d'avoir un système parallèle qui lui convient mieux, compatible avec celui de ses correspondants. L'éducation est donc la priorité. Mieux vaut un système à priori moins sur mais plus facile a auditer qu'un système "clé en main" facile à éviter.
2. Propositions de contacts : Les systèmes de chat généralistes (non spécifiques aux enfants) ont en général une fonction qui évite de recevoir des demandes de contact spontanées. Cette fonction très utile peut être activée pour les enfants comme les adultes.
3. Audit du web : Un audit très simple mais toujours utile consiste à rechercher dans votre moteur de recherche favori le nom de votre enfant, le numéro de téléphone qu'il utilise .. et voir ce qui est trouvé. Idéalement rien puisque ce qui le concerne devrait être privé (éventuellement des résultats sportifs).
4. Audit local : Vous pouvez procéder de même avec les dialogues chats privés de votre enfant. Certains logiciels de chat permettent d'enregistrer le contenu des conversations sur le disque pour recherche ultérieure. Compte tenu du temps moyen passé à chatter par des enfants et adolescents, espérer lire toutes les conversations est illusoire (en dehors des considérations éthiques).
5. Bloquer les fuites d'informations : Les logiciels qui reposent non pas sur l'audit mais sur l'empêchement est mis en avant par des associations de protection de l'enfance. Ces logiciels regardent en permanence ce qui est transmis dans votre navigateur par exemple et affiche une alerte des que certains mots clés que vous aurez définis sont transmis (nom de famille, numéro de tel, adresse, ...) et les bloque.
   Ce système est utile au tout début, lorsque le jeune internaute fait ses premiers pas autonomes sur internet, l'équivalent d'une paire de petites roues. Mais il est facilement à contourner, volontairement ou pas. Il n'a pas pour but d'interdire efficacement

mais d'avertir contre une divulgation irréfléchie dans les cas les plus simples. Il est un complément pédagogique à l'action éducative sur la seconde règle.

6. Vouloir "bloquer les pédophiles" : Les pédophiles ne sont pas différents sur internet des autres internautes, comme ils ne sont pas différents dans la rue des autres passants. ils ne viennent pas d'une adresse ou d'un site en particulier il est donc illusoire de vouloir les filtrer techniquement. Si les pédophiles étaient faciles à filtrer ils seraient facile à appréhender. Les deux actions utiles consistent d'une part à refuser le contact initial, d'autre part à limiter la divulgation d'informations une fois que le contact est initié.

# Chapitre 3

# Dangers psychologiques personnalisés

## 3.1 Être harcelé par des proches

**Danger :**

Ce phénomène est souvent désigné par son nom anglais "cyberbullying", ou harcèlement sur internet. Il s'agit par exemple de l'équivalent sur internet de la propagation d'une rumeur sur un collègue de classe ou d'une agression physique.

**Spécificité d'internet :**

La pratique existe dans les cours d'école depuis toujours, y compris sous la forme de violences physiques, mais l'anonymat et la rapidité des échanges sur internet démultiplie le mécanisme. Même si la violence n'est pas physique, les conséquences peuvent être très graves.

De nouvelles formes peuvent associer les formes électroniques et physiques, par exemple le "happy slapping" consiste à filmer une agression gratuite en groupe (typiquement une forte gifle donnée par surprise) avec un téléphone mobile et la diffuser sur internet ou de téléphone en téléphone. Internet est un média de mémoire même si la production se fait souvent dans l'instantané : la blessure de la gifle restera tant que la vidéo circulera, et pourra même s'emplifier au fur et a mesure de sa dissémination.

**En pratique :**

Pour les parents et encadrants, savoir que cela existe et être vigilant sur certains comportements. Une gifle dans une cours de recréation n'est pas qu'une simple gifle si elle est filmée par des complices, et mérite un traitement particulier.

Le fait qu'un groupe montre un contenu sur un portable et qu'une personne cherche désespérément à les empêcher doit vous faire supposer qu'il s'agit d'un cas de harcèlement. Sur internet la détection de rumeurs est moins évidente pour des tiers, mais le dialogue peut aider à comprendre qu'un adolescent est victime de harcèlement si vous êtes alerté sur les formes spécifiques à internet. Tout est question de mesure : un commentaire négatif isolé sur un blog ne constitue pas un harcèlement généralisé.

## 3.2 Être harcelé par un inconnu

### Danger :

Moins fréquent chez les enfants, il est possible d'être attaqué par un inconnu qui ne soit pas de son cercle proche, ou qui le soit mais agisse de manière anonyme.

### En pratique :

Bloquer les commentaires sur son blog, et bloquer la possibilité dans votre chat d'être contacté par des inconnus.

Pour les sites qui ne dépendent pas de vous, il est souvent possible de demander le retrait à l'héberger du site par simple demande précisant clairement quel contenu doit être enlevé et ce même sans porter plainte contre l'héberger. Ceci peut typiquement se faire depuis le site lui même ou par envoi d'un courrier.

Demander à l'héberger une plateforme sociale de cesser toute atteinte contre vous par des tiers revient a demander à votre opérateur téléphonique qu'il fasse cesser tous les commérages entre tiers faits lors d'appels sur son réseau, c'est impossible.

## 3.3 Pour des mineurs âgés, échanger des photos d'eux même

Voici un cas ou les dérives sont très fréquentes, mais ou les victimes se mettent elles même en danger sans en imaginer les conséquences (légales et psychologiques).

### Danger :

Deux amants de 17 ans (ayant atteint la majorité sexuelle, sexuellement actifs ou pas) se prennent en photo nus ou presque sur leur téléphone portable.

1. Premier cas (peu fréquent mais réel) : Soit il n'y a pas propagation et le média reste entre les deux amants. Ceci est légalement (dans certains pays et suivant le contexte) considéré comme de la production, possession et distribution de matériel pedopornographique, très gravement puni et qui est extrêmement stigmatisant. Ceci même si la relation sexuelle consentie des deux mêmes personnes sera elle rarement punie. Les juges à l'origine de ces poursuites ne considèrent pas forcement qu'il s'agit de pédopornographie mais sont sans doute tentés d'utiliser cette arme légale pour freiner la sexualité des adolescents. Si les deux adolescents sont en voyage scolaire à l'étranger, se souvenir que les douaniers ont dans certains pays le droit de fouiller vos contenus numériques (et qu'ils le font).
2. Deuxième cas (fréquent) : Un des deux pour un motif quelconque (vengeance après une rupture, amusement) ou un tiers qui accède au mobile, propage sur internet ou de mobile en mobile le contenu. Ceci est pénalement encore plus grave que le cas précèdent dans la mesure ou le média a été propage de manière non personnelle sur un réseau public. Pour une blague de mauvais goût (et très choquante pour la victime), les conséquences pénales sont beaucoup plus graves que ne l'imaginaient leur auteurs.

**Règle absolue :**

Ne jamais se laisser prendre en photo, filmer ou voir en webcam (qui peut être enregistrée) dénudé, même et surtout si c'est par un proche, comme au sein d'un couple d'adolescents. Ce pas forcement pour des raisons morales mais pour de très bonnes raisons légales et pour éviter les propagations incontrôlées.

Et ne surtout pas propager, entrer en possession ou visionner un tel contenu. si vous ne le faites pas par respect, faites le par peur la aussi des conséquences légales.

## 3.4 Voir les photos/vidéos de mineurs propagées à des tiers

**Danger :**

Un pédophile entre en possession de photos ou vidéos de vos enfants, sans en connaître l'origine donc sans danger direct pour eux.

Ceci peut arriver dès que des contenus numériques sont partagés de manière non confidentielle. Par exemple des photos de vos enfants postées sur votre blog, ou même votre profil Facebook. En effet le mode par défaut autorise la consultation partielle de vos photos par des tiers non amis. Le danger de voir vos photos récupérées est réel, la collecte automatique de photos sur internet est très courante. Une fois les photos sorties de votre cadre privé, elles sont disponibles pour toute utilisation incontrôlée, par exemple pédophile. La probabilité est minime mais réelle.

**En pratique :**

Par principe ne pas poster de photos d'enfants sur internet sauf si vous avez un accès protégé par mot de passe qui restreint réellement l'accès à vos proches. Considérer des médias sociaux tels Facebook comme semi publics et pas comme privés.

# Chapitre 4

# Dangers psychologiques non ciblés

## 4.1 Voir des contenus de pornographie enfantine à son insu

**Danger :**

Les sites et contenus de pornographie adulte sont très fréquents mais n'ont pas pour vocation de produire et diffuser de la pornographie enfantine. Les sites de pornographie réellement enfantine sont eux surtout cachés et confidentiels. Le danger reste très donc théorique.

Par contre des producteurs de pornographie peuvent employer des acteurs majeurs classiques pour les faire jouer le rôle d'un tout juste majeur (légal) ou presque majeur (illégal). Le concept vaut aussi pour des bandes dessinées, dessins et animations 3D selon la culture du pays (Japon par exemple).

Ceci dit, les contenus de pornographie enfantine illégaux et adultes contrefaits peuvent se retrouver en même temps sur un réseau de partage de fichiers contrefaits (même si ils y sont places par des internautes distincts) et être téléchargés sur l'ordinateur d'un internaute qui ferait une présélection peu précise de ses fichiers à télécharger.

**Spécificité d'internet :**

Dans la mesure ou un adolescent passe en moyenne 1h40 (selon certaines sondages) par semaine à regarder et chercher des contenus pornographiques (contrefaits ou pas, légaux ou pas), la probabilité de rencontrer des contenus sortant du cadre légal français sans qu'il le souhaite est non négligeable, le sujet mérite donc d'être évoqué.

La contrefaçon n'influe pas sur la capacité à trouver (à son insu ou pas) des contenus de pornographie infantile puisque les médias contrefaits ont forcement été approuvés pour une distribution légales avait d'être contrefaits. La spécificité d'internet repose surtout dans le fait de consommer des médias étrangers (contrefaits ou pas) dont la classification est différente et des médias crées par des particuliers.

**En pratique :**

La possession de matériel pédopornographique, même sans intention de le consulter, est fortement répréhensible. Il convient donc aux internautes cherchant des contenus pornographiques adultes (contrefaits ou pas) de faire attention à leurs termes de recherche,

ne pas utiliser des systèmes de téléchargement automatiques (type podcast) dans ce cadre. L'utilisation de systèmes de mutualisation des risques comme des peer2peer indirects sont aussi à proscrire pour ne pas favoriser le transfert par son ordinateur de médias certes aussi illégaux que les vôtres mais beaucoup plus graves.

Ce dans le double but de ne pas s'exposer à des poursuites sévères, mais aussi et surtout pour ne pas "noyer" les contenus pédopornographiques dans la masse gigantesque des contenus pornographiques adultes, et faciliter le travail d'identification des réels contenus pédopornographiques, leur auteurs et consommateurs.

**Technique :**

La consultation de sites de pédopornographiques est répréhensible mais techniquement possible, aussi certains législateurs aux nobles intentions proposent de bloquer des sites ouvertement pédophiles à l'accès sur tout le territoire par une "liste noire" de plusieurs milliers de sites.

Or la consultation en longueur de ces sites ne se fait pas par hasard mais par choix. La consultation par erreur de contenus pédopornographiques se fait lorsque ces contenus sortent justement de ces sites ouvertement pédopornographiques. Leur blocage ne sera pas utile pour limiter la consultation "par erreur".

Ce mécanisme de "liste noire" aurait pour effet collatéral involontaire de faire croire aux parents peu technophiles que ce sont les pédophiles qui sont bloqués d'internet alors que ce sont des sites pédophiles qui le sont, créant une illusion de sécurité dangereuse.

Second effet collatéral, la recherche des forces de l'ordre serait complexifiée. Les sites bloqués au niveau national seraient aussi bloqués à la consultation pour tous les pédophiles. Or les unités d'enquête utilisent certains sites d'échanges entre pédophiles pour entrer en contact avec eux. En effet le but prioritaire des enquêteurs n'est pas d'empêcher les médias de circuler mais de retrouver les auteurs et les victimes. Certains pédophiles peu technophiles utilisent pour l'instant des techniques de communication peu sures qui permettent aux enquêteurs de les contacter. Bloquer ces moyens les poussera vers des moyens beaucoup plus confidentiels (qui existent).

De plus se pose le problème de la définition de la liste : ces sites ont en effet un grand nombre d'adresses et en changent constamment. La liste ne servirait qu'a garder un historique de leurs adresses passées.

## 4.2 Voir des contenus choquants à son insu

**Danger :**

Un internaute cherche un contenu innocent et je trouve des références à des contenus choquants compte tenu de son âge ou sa sensibilité. C'est possible s'il sous estime les résultats potentiels de sa recherche : un enfant qui cherche des informations sur la guerre pour ses études et qui trouve en réponse le site d'Amnesty International sur les enfants soldats peut être choqué.
Autre exemple : un enfant consulte un grand quotidien national sur lequel lui est présenté la mise en ligne de 50 ans de magazine Playboy, ou la partie sexualité du journal, spécifique

au journal en ligne.
De plus un mot peut avoir plusieurs sens que l'on ignore ou un sens différent en fonction des sensibilités culturelles.

### Spécificité d'internet :

Internet ne propose pas forcement des médias plus adultes par nature que le monde réel, mais leur accès est plus facile. Un enfant ira rarement acheter un quotidien national par lui même, alors qu'il ira plus facilement sur son site web.

Il reste toujours le cas d'un adulte qui montre ou donne accès à un contenu pornographique à un mineur dont l'âge ne correspond pas à la signalétique. Mais pas de spécificité d'internet si ce n'est que des contenus potentiellement illégaux en France sont disponibles en ligne, et sans signalétique.

La signalétique sur internet des contenus (légaux ou contrefaits) se réduit généralement à pornographique ("XXX") ou pas.

### En pratique :

Les moteurs de recherche cachent typiquement par défaut une catégorie de contenus (option "safesearch" de Google). Le tri, assez efficace mais imparfait, est un mix de liste noire et d'analyse contextuelle. Par contre le filtre a plus pour but de ne pas montrer des contenus pornographiques ou extrêmes que potentiellement choquants.

L'exposition la plus fréquente à de la pornographie non voulue concerne la publicité intrusive ou "spam". Cette publicité est reçue par email et vante des sites pornographiques en général basés à l'étranger. Et ce même si vous n'avez jamais fréquenté ces sites, ni jamais demandé à les recevoir. Le contenu est parfois très cru.

Très fréquent aussi, les virus "pop-ups". Certains virus informatiques sont capables de prendre le contrôle de votre ordinateur et ont pour but principal de générer des revenus publicitaires à leur auteur en montrant des publicités (typiquement pour de la pornographie ou des paris illégaux en ligne). Une fois votre ordinateur infecté il affichera à sa guise des publicités sur votre écran. Ces hackers et leurs partenaires commerciaux sont eux aussi rarement en France.

### Technique :

Pour en protéger un très jeune enfant, le système de contrôle parental par liste "blanche" est efficace mais très restrictif : seuls les sites sur la liste pourront être consultés. Wikipedia va par exemple être systématiquement bloqué.

Pour les moteurs de recherche, l'option est activée par défaut.

Pour le spam, ne pas publier son adresse email sur aucun site, avoir un bon filtre anti-spam (souvent dépendant de votre fournisseur de mail). Ces spammeurs et leurs partenaires sont rarement en France, une action juridique serait peu efficace.

Certains systèmes d'exploitation sont plus vulnérables que d'autres, mais avoir un bon anti-virus à jour aide beaucoup (certains sont gratuits).

Vouloir bloquer l'accès a des contenus de type pornographique à un adolescent est totalement illusoire. D'une part parce que sa motivation est grande (1h40 en moyenne par semaine), d'autre part parce que son niveau d'expertise technique dépasse largement les capacités de logiciels et matériels.

**Vraie fausse alerte :**

Passons maintenant à un cas devenu plus rare mais assez troublant. Sur des sites de peer2peer sont disponibles entre autres des contrefaçons de films, y compris de films destinés aux jeunes enfants comme des dessins animés.

Des personnes mal intentionnées proposaient de très nombreuses versions de ces films dont le montage vidéo avait été altéré pour inclure des passages de pornographie adulte. Ces personnes avaient sans doute envie de nuire aux enfants des contrefacteurs ou un intérêt plus précis à voire associer dans l'esprit collectif les contrefacteurs à la pornographie. Ces arguments on même été repris au parlement récemment.

Quoi qu'il en soi, ces personnes anonymes continuent à altérer les montages et proposer des versions altérées pour gêner les contrefacteurs, mais maintenant sans inclusion de matériaux potentiellement choquants. D'une manière générale, les clubs informels de contrefacteurs qui formatent et postent (bénévolement) l'essentiel des contrefaçons sont souvent des maniaques de la classification, de l'étiquetage des contenus, et la valorisation des contenus correctement formatés. Il est certes possible de regretter une telle expertise technique dans la contrefaçon, acte illégal, mais l'avantage collatéral en ce qui nous concerne est que le déchargement de contenus choquants est souvent clairement mis a part par un label "XXX".

## 4.3 Voir des contenus choquants après demande

**Danger :**

Un internaute consulte un contenu qu'il trouve choquant après l'avoir cherché en sous estimant sa capacité d'assimilation. Le principe est qu'un mineur n'a pas forcement le recul à la hauteur de sa curiosité.

**Spécificité d'internet :**

Contrairement à d'autres médias, sur internet l'internaute est actif et doit positivement chercher un contenu pour le visionner. L'anticipation permet donc de mieux absorber et le caractère actif permet de ne pas rester passif et zapper.

Comme dans les médias Français, qui ont une signalétique à plusieurs niveaux, internet a une signalétique qui est elle typiquement à un niveau. Beaucoup de sites de pornographie adulte ont un système pour demander l'âge de l'internaute, mais ce mécanisme est purement déclaratif. D'autres ont un système qui demande l'entrée d'un numéro de carte bleue sans paiement (prétendent ils).

Il existe un second niveau, dit ”pas sur pour le bureau”. Ce niveau est destiné non pas à prévenir l'internaute lui même mais de le protéger des regards de ses collègues dans le contexte d'un bureau partagé.

# Chapitre 5

# Lutte contre la pédopornographie et la pornographie

## 5.1 Définir les objectifs

### 5.1.1 Pédopornographie ou pornographie ?

Il peut sembler étrange de parler en même temps de pornographie et pédopornographie, alors que l'un est un divertissement légal (dans un cadre bien précis) et l'autre totalement illégal. Mais l'un est parfois partiellement interdit en prenant l'autre comme alibi, de plus dans un internet globalisé un contenu tout a fait légal dans un pays peut être non seulement illégal mais aussi considéré comme inacceptable dans un autre.
Il convient donc de bien prendre en compte les limites de chaque pratique, établir clairement ses objectifs et éventuellement adapter la pratique à des contenus non Français.

### 5.1.2 Lutter contre les sites pédopornographique ou les pédophiles ?

La loi française permet des poursuites dans un cadre assez large en laissant le juge libre d'interpréter en fonction du contexte. De plus les intermédiaires techniques fiançais (hébergeurs, fournisseurs, ...) sont traditionnellement prêts à appliquer les décisions d'un juge avec beaucoup d'attention.

La loi ne se focalise pas sur le fait d'être ou pas pédophile ce qui nécessiterait une expertise médicale complexe à réaliser dans le consentement du sujet, mais sur les contenus pédopornographique (création, recel, consultation, ...) plus faciles à caractériser.
Mais le but premier des enquêteurs est avant tout la protection des victimes et la prévention des actes. Aussi la pédopornographie est un moyen d'atteindre et condamner des pédophiles plus qu'une fin en soi.
Il est techniquement possible de bloquer un grand nombre de sites pédopornographiques au niveau national, provoquant un repli des pédophiles sur des moyens de communications moins voyants et beaucoup plus sécurisés pour eux.
Ne pas les bloquer pose le problème de l'impunité, c'est pour cela que l'objectif doit être clairement établi : la priorité est elle à la lutte contre les pédophiles et la création de contenus ou bien la lutte contre la diffusion de pédopornographie ?

Il existe des moyens d'utiliser les médias pédopornographiques pour retrouver les auteurs et clients, dont certains ne sont pas encore légaux ou mis en pratique.

## 5.2 Spécificité d'internet

### 5.2.1 Web 1.0

En ce qui concerne la spécificité d'internet, la loi reste très vague sur les détails techniques et le concept d'internet 1.0 et de réseau social sont finalement bien couverts par la description "diffusion de l'image ou de la représentation du mineur à destination d'un public non déterminé, un réseau de communications électroniques".

### 5.2.2 Web 2.0

#### Cloud

Les sites d'échanges pédophiles leur permettent d'échanger comme n'importe quel site de minorité peu visible permet de se fédérer. Sans entrer trop loin dans les détails, la loi a bien pris en compte la notion de "cloud" ou les contenus sont stockés en ligne et non pas localement chez le pédophile. Aussi le texte "le fait de consulter habituellement un service de communication au public en ligne mettant à disposition une telle image" est un exemple de loi qui s'applique bien à internet et à ses évolutions sans être pour autant trop technique.

#### Sites généralistes à usage personnalisé ?

Cependant elle repose sur l'idée qu'un service est dédié à un usage, ce qui dans le cas spécifique de la pedopornographique semble encore être le cas compte tenu de la lutte forte des sites généralistes contre les pédophiles. En pratique des médias stockés sur un serveur. Mais la consultation régulière de second life ou facebook, sites généralistes, avec des microconsultations ponctuelles et furtives de pédopornographie est elle couverte ?

#### Social

La notion de "bande organisée" demande à être un peu détaillée, à l'heure ou les sites sociaux se multiplient. Les "amis" sur facebook sont ils une bande ? Le post d'informations ou médias à tous ses amis alors que ceux ci ne la consulteront peut être pas est elle une communication publique ou privée ?

### 5.2.3 Territorialité

#### Import Export

La notion d'import/export est elle beaucoup plus complexe puisque la localisation géographique de serveurs ou correspondants est souvent inconnue, et elle incrimine potentiellement un hébergeur sincèrement innocent dont l'infrastructure serait internationalisée et flexible.

#### Hébergement

D'un autre cote l'hébergement à l'étranger reste encore impuni, y compris dans des pays comme les États-Unis ou la liberté d'expression sert de rempart. Améliorer la coopération internationale pour retrouver les auteurs de ces sites est bien sur utile mais complexe, aussi en attendant utiliser ces sites comme des pièges serait beaucoup plus productif.

#### Tracer la consultation

Après tout, un FAI français très coopératif peut facilement retrouver qui accède un site donné par son DNS, pour peu que le pédophile n'utilise pas des contre-mesures sophistiquées. Une résolution DNS ne saurait être suffisante pour incriminer un individu, mais pour chercher plus loin oui.

#### Universalité d'internet

Internet, de par son cote objectivement universel, pourrait être un bon motif pour se doter d'une compétence universelle. Qu'un américain héberge ouvertement des contenus pédophiles est souvent considéré comme légal sur son territoire, mais son action a une portée mondiale et permanente. Qu'il le fasse depuis la France ou les États-Unis a la même portée, que l'on considère le contrôle éditorial ou même l'hébergement, celle ci dure tant que le contenu est en ligne. Aussi pourrait il se voir poursuivi a l'occasion d'un passage de frontière.

### 5.2.4 Diversité des médias

Si un texte fait encore référence a des "cassettes", des termes très neutres techniquement sont utilisés. Ils englobent des formes diverses et répondant à des cas très concrets comme des avatars 3D de jeux vidéos ou jeux de rôles en ligne.

## 5.3 Mesures techniques

### 5.3.1 Liste noire nationale

En dehors du fait de définir clairement la stratégie et l'utilisation qui peut être faite de ces sites pour trouver et incriminer des pédophiles, il est possible si tel est le but souhaite et moyennant la collaboration des FAIs de bloquer une liste de sites au niveau national.

Ceci pose cependant quelques problèmes techniques :

#### Définition de la liste

Une liste initiale d'adresses peut être définie assez facilement par un groupe d'experts. Cependant les sites peuvent avoir plusieurs adresses nominatives très facilement. Si tel est leur intérêt ils le feront quotidiennement. L'ajout de nouvelles adresses se révélera une tache lourde et peu efficace. Le blocage d'adresses au niveau DNS est relativement facile a mettre en place.

Si le blocage est implémenté au niveau IP (ce qui est déjà plus complexe a mettre en place) le même concept s'applique si l'hébergeur est complice, ce qui semble être le cas dans le cas de sites très visibles. Il faudra alors bannir tout la classe d'IPs que l'hébergeur complice peut utiliser, donc tous les serveurs qu'il a dans son datacenter.

#### Contournement

Il est fort probable que des pédophiles ont une très forte motivation, qu'ils n'arrêteront pas pour autant de consulter de la pédopornographie si c'est techniquement possible.

Si le blocage DNS intervient en modifiant des entrées dans le serveur du FAI, la mesure sera contournée en utilisant un autre serveur DNS étrangers standards. La mesure est très simple à effectuer et ne constitue pas le signe d'une activité illégale en soi.
Ce contournement n'empêche pas en soi le traçage, mais il est probable que le pédophile qui commence à s'intéresser à des mesures de contournement aille plus loin que ce simple contournement et adopte des mesures qui empêchent complètement le traçage. Commencer une escalade technique entre enquêteurs et pédophiles est dangereux car à ce jeu la les enquêteurs même avec de grandes compétences techniques et des moyens ne pourront attraper que les plus novices des pédophiles.

Si la mesure est implémentée au niveau du routage, (plus complexe), le contournement passera par l'usage de proxys anonymisants ou de VPNs avec des serveurs à l'étranger. Tout comme les serveurs DNS l'usage de serveurs VPN étrangers ne constitue pas en soi une preuve d'action illégale, ni ne devrait lever de suscitions.

#### Évitement

Ces deux contournements sont des astuces techniques pour continuer à accéder au même service comme défini sur la liste, mais la mesure la plus simple et surtout la plus efficace pour éviter toute suscition est l'évitement. Utiliser un autre service dédié à la pédopornographie d'abord, puis si le blocage se répète passer à un service généraliste qui ne sera lui jamais bloqué. Le passage sur un service généraliste s'accompagnera d'une grande précaution et compartimentation qui limitera fortement le travail des enquêteurs.

### 5.3.2 Filtre contextuel

Il est également possible d'implémenter un filtre contextuel, par exemple en altérant les résultats des moteurs de recherche. Ils le font certes déjà d'eux même avec une liste de sites sur liste noire interne mais il est possible d'aller plus loin. Des mots qui seraient innocents pris à part mais bloqués lors d'une recherche croisée.

Clairement plus fastidieuse à mettre en place, cette mesure ne serait utile que peu de temps. Les pédophiles sont à priori motivés et connectés en un réseau à multiple points de contacts et rapidement mouvant. Bloquer un aspect provoque une résistance rapide en retour grâce à l'utilisation d'un autre point de contact et l'échange d'informations. Le problème peut en soi se comparer en médecine à la multirésistance après un usage unitaire d'antibiotiques.

En Chine par exemple, les internautes utilisent d'autres mots que ceux bloqués, totalement innocents pour désigner les mêmes concepts. Il leur a suffit de s'organiser de manière informelle en réseau. Sur les réseaux newz de contrefaçons de films, le numéro d'identification sur allocine sert à poster des contenus pour qu'ils ne soient pas repérés par des filtres contextuels.

### 5.3.3 Filtre local sortant

En terme technique, un "proxy local" (pour simplifier).
Ce type de logiciel est typiquement installé sur un poste client, ou requiert une simple modification des réglages de votre navigateur. Il va typiquement faire appel a un service

distant comme référence de filtrage. (Nombre de logiciel de protection parentale se contentent en fait de changer le proxy de votre navigateur, rien de plus) Le but est d'empêcher la consultation de certains sites ou de faire sortir certaines informations.

Le modèle d'usage typique dans notre contexte est de limiter la sortie d'informations par un enfant très jeune qui ne maîtrise pas bien les conséquences de son acte. Mais les logiciels sont typiquement très limités, ne bloquant par exemple pas votre chat favori mais seulement le navigateur ... pour les plus petits donc. Le concept ne fonctionne pas pour bloquer un pédophile contre lui même puisque celui ci est maître de sa machine, et qu'il peut potentiellement comprendre les astuces techniques de contournement.

### 5.3.4 Filtre local entrant

En terme technique, un "firewall" (encore pour simplifier).
Le terme de mur de feu est en fait mal choisi, car le logiciel étant sous votre contrôle sur votre machine, il a surtout pour but de vous protéger contre des intrusions extérieures ou contre l'import de contenus extérieurs potentiellement nocifs.
En pratique, ils sont utilisés pour la protection contre différentes formes de virus. Ces logiciels ne peuvent lutter contre votre volonté d'accéder à ce que vous voulez. Si je choisis d'inclure mon virus dans une archive avec un mot de passe, le firewall sera bien obligé de me faire confiance.

## 5.4 Le mythe de la grande muraille

Il est tentant de vouloir procéder sur le modèle de la grande muraille électronique de Chine. En fait de muraille, le système inclus des proxys obligatoires et transparents, des blocages par IP, par DNS, contextuels par mots clés et surtout une armée de censeurs.
Ce serait se tromper d'objectif. Le système chinois a pour but de réduire la contestation et la liberté d'expression à l'échelle du pays, de la population en moyenne, pas d'interdire des comportements uniques.
La volonté de pays comme la France est différente. Le but est de cibler des comportements précis d'individus très motivés.

Un internaute chinois simplement motivé trouvera les informations techniques pour surfer à sa guise en passant outre toutes les mesures techniques. Les filtrages par mots clés sont devenus la risée des internautes moyens qui se font un plaisir de les contourner.
Comment imaginer qu'un pédophile très motivé se laissera bloquer dans sa consultation alors que des contre mesures techniques existent ?

La ou la Chine a raison de maintenir sa muraille, c'est que l'effet moyen sur la population est semble t il positif (compte tenu de ses objectifs). Les internautes ont moins de moyens de communiquer librement, et l'auto censure s'est installée. Passer outre requiert une certaine motivation que la population moyenne n'a pas.
La France ne cherche pas un effet moyen sur la population, qui est déjà fortement anti pédopornographie, mais sur une toute petite minorité d'individus très motivés.

Avec la meilleure volonté du monde la France avec son muret n'égalera jamais la Chine avec sa mythique grande muraille. Et quand bien même elle tenterait les pédophiles seraient toujours aussi pédophiles et trouveraient les contre mesures.

# Chapitre 6

# Code Pénal

## 6.1 CP 227-24 (Violence ou pornographie vue par un mineur)

Le fait soit de fabriquer, de transporter, de diffuser par quelque moyen que ce soit et quel qu'en soit le support un message à caractère violent ou pornographique ou de nature à porter gravement atteinte à la dignité humaine, soit de faire commerce d'un tel message, est puni de trois ans d'emprisonnement et de 75000 euros d'amende lorsque ce message est susceptible d'être vu ou perçu par un mineur.
Lorsque les infractions prévues au présent article sont soumises par la voie de la presse écrite ou audiovisuelle ou de la communication au public en ligne, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables.

## 6.2 CP 227-23 (Pornographie représentant des mineurs)

Le fait, 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 est puni de cinq ans d'emprisonnement et de 75 000 Euros d'amende.
Le fait d'offrir, de rendre disponible ou de diffuser une telle image ou représentation, par quelque moyen que ce soit, de l'importer ou de l'exporter, de la faire importer ou de la faire exporter, est puni des mêmes peines.
Les peines sont portées à sept ans d'emprisonnement et à 100 000 Euros d'amende lorsqu'il a été utilisé, pour la diffusion de l'image ou de la représentation du mineur à destination d'un public non déterminé, un réseau de communications électroniques.
La tentative des délits prévus aux alinéas précédents est punie des mêmes peines.
Le fait de consulter habituellement un service de communication au public en ligne mettant à disposition une telle image ou représentation ou de détenir une telle image ou représentation par quelque moyen que ce soit est puni de deux ans d'emprisonnement et 30000 euros d'amende.
Les infractions prévues au présent article sont punies de dix ans d'emprisonnement et de 500 000 Euros d'amende lorsqu'elles sont commises en bande organisée.
Les dispositions du présent article sont également applicables aux images pornographiques d'une personne dont l'aspect physique est celui d'un mineur, sauf s'il est établi que cette personne était âgée de dix-huit ans au jour de la fixation ou de l'enregistrement de son image.

## 6.3 CP 227-22 (Corruption de mineurs)

Le fait de favoriser ou de tenter de favoriser la corruption d'un mineur est puni de cinq ans d'emprisonnement et de 75000 euros d'amende. Ces peines sont portées à sept ans d'emprisonnement et 100000 euros d'amende lorsque le mineur est âgé de moins de quinze ans ou 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 communications électroniques ou que les faits sont commis dans les établissements d'enseignement ou d'éducation ou dans les locaux de l'administration, ainsi que, lors des entrées ou sorties des élèves ou du public ou dans un temps très voisin de celles-ci, aux abords de ces établissements ou locaux.
Les mêmes peines sont notamment applicables au fait, commis par un majeur, d'organiser des réunions comportant des exhibitions ou des relations sexuelles auxquelles un mineur assiste ou participe.
Les peines sont portées à dix ans d'emprisonnement et 1 000 000 Euros d'amende lorsque les faits ont été commis en bande organisée.