La lutte contre les contenus illégaux sur Internet

Conférence Barreau de Paris « Régulation : filtrage ou internet civilisé ? »

Patrick Maigron
Enseignant-chercheur / Ingénieur d'études
Institut Télécom / Télécom SudParis
patrick.maigron@telecom-sudparis.eu

23 novembre 2011

Plan

- **Quels contenus illégaux ?**
- **Pourquoi connaître les techniques de lutte ?**
- **Comment lutter contre les contenus illégaux ?**
  - Suppression des contenus à la source
  - Saisie des noms de domaine
  - Filtrage : par l'adresse IP, par le nom de domaine, par l'URL, par le contenu (DPI), hybride
- **Mise en œuvre du filtrage**
- **Inconvénients du filtrage**
- **Contournements possibles**
- **Efficacité du filtrage**
- **Conclusion**

Quels contenus illégaux ?

- **Types de contenus illégaux**
  - Atteinte aux droits d'auteurs et aux droits voisins
    - Audio/vidéo/logiciels
  - Diffusion de produits de contrefaçon
  - Jeux d'argent et de hasard en ligne illégaux (ARJEL)
    - StanJames.com (2010), 5Dimes.com (2011)
  - Diffusion d'images ou de représentations de mineurs / pédopornographie (LOPPSI2)
  - Diffusion de propos racistes, négationnistes…
    - Vente d'objets nazis sur Yahoo! (2000), site AAARGH (2005)
  - Diffamation, injure
    - Copwatch (2011)
  - Tout contenu occasionnant un dommage (LCEN)
  - Mais aussi les contenus présentant des risques pour la sécurité informatique (spam, virus, attaques par déni de service)

Pourquoi connaître les techniques de lutte contre les contenus illégaux ? (1/2)

- **Le juge n'a pas nécessairement besoin de choisir lui-même une technique de lutte**
  - Exemples : affaires StanJames.com et 5Dimes.com

Enjoignons aux sociétés […] de mettre en œuvre ou faire mettre en œuvre, sans délai, toutes mesures propres à empêcher l'accès, à partir du territoire français et/ou par leurs abonnés situés sur ce territoire, au contenu du service de communication en ligne de la société Fivedimes accessible actuellement aux adresses […]

– Ordonnance rendue en la forme des référés, TGI Paris, 28 avril 2011

Pourquoi connaître les techniques de lutte contre les contenus illégaux ? (2/2)

- **Mais il peut avoir besoin de connaître les limitations et les contraintes inhérentes à ces techniques de lutte**
  - Exemple : affaire Copwatch

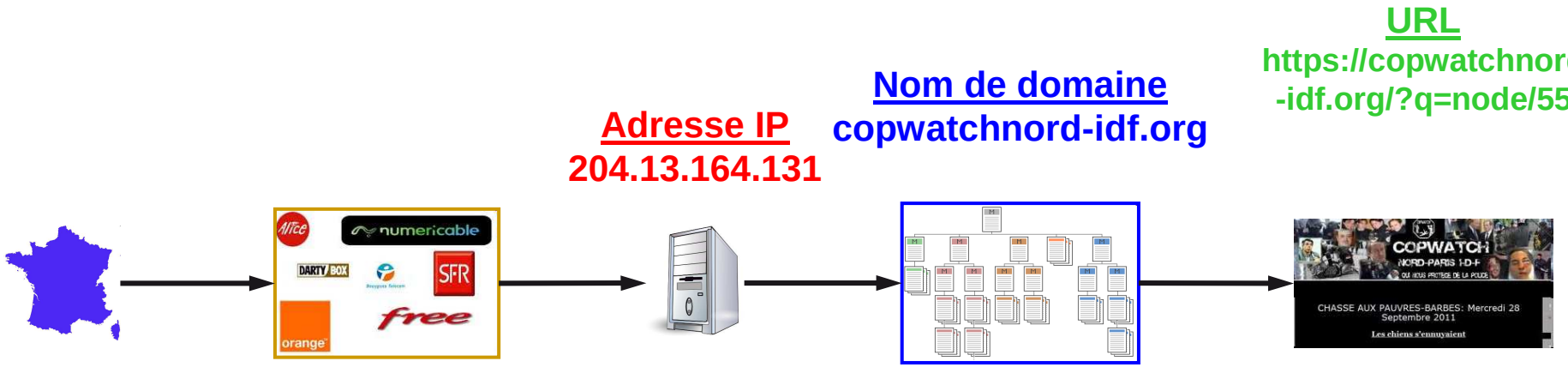
Attendu […]
Que toutefois, ce système nécessite l'acquisition d'ordinateurs « Deep Packet Inspectors » […] ;
que […] chaque fournisseur au réseau internet français se trouverait contraint de faire l'acquisition de […] ;
que par ailleurs, la mise en place d'une telle mesure serait de l'ordre de six mois à un an ;
qu'enfin […] l'analyse du contenu des requêtes […] pose une difficulté liée à la protection des libertés individuelles ;

Le Tribunal […] FAIT injonction aux sociétés […] de mettre en œuvre ou faire mettre en œuvre, sans délai, toutes mesures propres à empêcher l'accès, à partir du territoire français et/ou par leurs abonnés situés sur ce territoire, au site « https://copwatchnord-idf.org/ » - (blocage par IP ou blocage par DNS)

– Jugement en état de référé, TGI Paris, 14 octobre 2011

Comment accède-t-on aux contenus sur Internet ?

- **Un ensemble d'identifiants : adresse IP, nom de domaine, URL**



L'internaute accède à Internet par l'intermédiaire d'un fournisseur d'accès (FAI)

Le serveur est localisé chez un hébergeur web

Le site est identifié par un nom de domaine géré par un registre et un bureau d'enregistrement

Les pages sont identifiées par des URL

- **Un ensemble d'opérateurs techniques : FAI, hébergeur web, registre et bureau d'enregistrement du nom de domaine**

Comment lutter contre les contenus illégaux ?

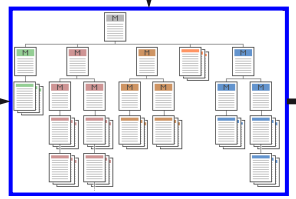
- **Saisir le nom de domaine**

Registre et bureau d'enregistrement

- **Supprimer les contenus à la source**

Hébergeur

Adresse IP
204.13.164.131



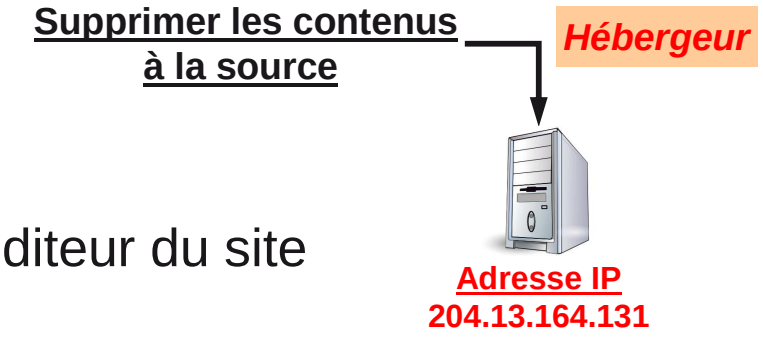
Nom de domaine
copwatchnord-idf.org

URL
https://copwatchnord-idf.org/?q=node/55

FAI

- **Filtrer à partir :**
  - **de l'adresse IP**
  - **du nom de domaine**
  - **de l'URL**
  - **du contenu des pages**

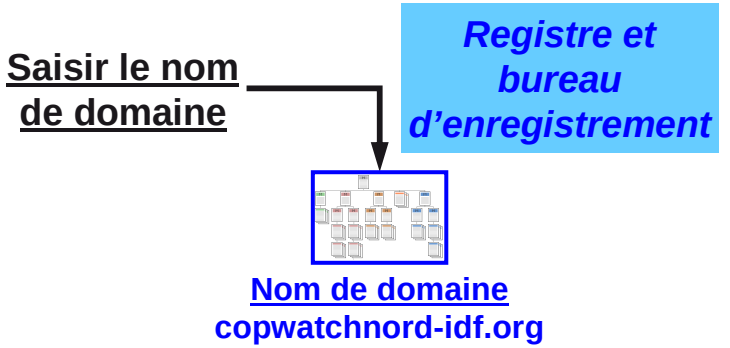
Suppression des contenus à la source



- **Procédure**
  - Identifier l'hébergeur fournissant l'adresse IP du site
  - Demander le retrait des contenus à l'éditeur du site ou à l'hébergeur
- **Difficultés de mise en œuvre**
  - L'hébergeur peut être hors de France
    - Copwatch : Riseup Networks (États-Unis)
  - Nécessité d'une coopération internationale
    - Les lois limitant la liberté d'expression sont variables selon les législations nationales
    - Accord sur un socle minimum de types de contenus justifiant d'une telle suppression ?
- **Contournement**
  - Par le site : changer d'hébergeur

Saisie du nom de domaine

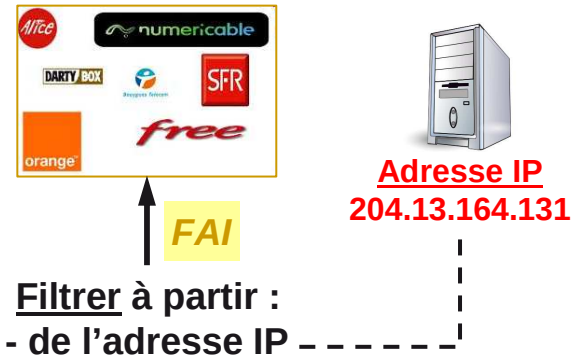
- **Procédure**
  - Identifier le registre et/ou le bureau d'enregistrement du nom de domaine
  - Demander la saisie du nom de domaine au registre ou au bureau d'enregistrement



- **Exemple**
  - États-Unis : saisie de noms de domaine associés à des sites de contrefaçon, de jeux en ligne et pour violation de droits de PI
    - « Operation in Our Sites », DoJ et service des douanes, depuis 2010
    - Lorsque le registre et/ou le bureau d'enregistrement est américain
- **Difficultés de mise en œuvre**
  - Le registre et le bureau d'enregistrement peuvent être hors de France
    - Copwatch : Gandi (France) → Gandi + FreeDNS (USA)
  - Nécessité d'une collaboration internationale
    - Travaux en cours à l'ICANN entre gouvernements et bureaux d'enregistrement
- **Contournement**
  - Par le site : utiliser un autre nom de domaine
    - Exemple : *rojadirecta.org* → *rojadirecta.es*

Filtrage sur l'adresse IP

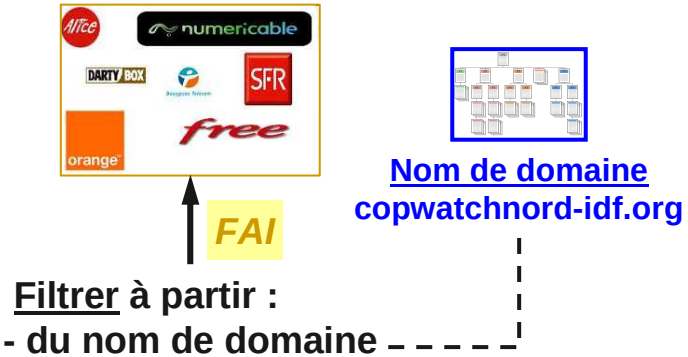
- **Procédure**
  - Demander aux FAI français de filtrer l'adresse IP du site
  - Les échanges entre les internautes et cette adresse IP sont bloqués (configuration des routeurs du FAI)



- **Exemple**
  - Copwatch filtré sur l'adresse IP par certains FAI
- **Contournement**
  - Par le site : changer son adresse IP (par exemple en changeant d'hébergeur)

Filtrage sur le nom de domaine

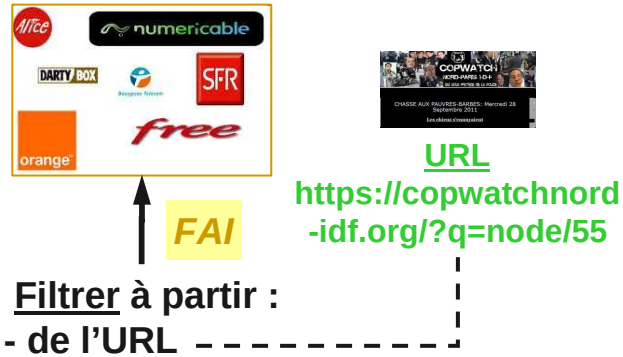
- **Procédure**
  - Demander aux FAI français de filtrer le nom de domaine du site
  - Les requêtes vers le nom de domaine ne renvoient plus l'adresse IP du site (configuration des serveurs DNS du FAI)



- **Contournement**
  - Par l'internaute : utiliser des serveurs DNS alternatifs à la place de ceux de son FAI
  - Par le site : utiliser un autre nom de domaine
    - Exemples : sites champignons utilisés pour la vente de produits de contrefaçon

Filtrage sur l'URL

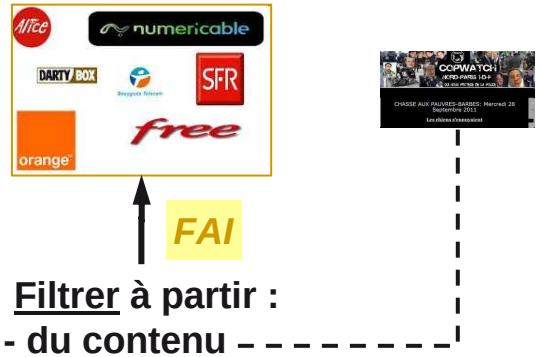
- **Procédure**
  - Demander aux FAI français de filtrer les URL des pages concernées
  - Les requêtes web vers ces URL ne renvoient plus les pages correspondantes (configuration d'un proxy web)



- **Difficultés de mise en œuvre**
  - Mise en place d'équipements de filtrage de type « proxy » plus coûteux et ralentissant le trafic
  - Difficultés supplémentaires en cas de trafic chiffré (HTTPS)
    - Exemple : *https://copwatchnord-idf.org*
- **Contournement**
  - Par le site : changer les URL des pages filtrées

Filtrage sur le contenu

- **Procédure**
  - Demander aux FAI français de filtrer le contenu des pages concernées
  - Les transferts de pages web contenant ces contenus sont bloqués (configuration d'un équipement DPI)
  - Possibilité de filtrer les données audio et vidéo à partir de tatouages numériques (watermarking)
- **Difficultés de mise en œuvre**
  - Mise en place d'équipements de filtrage de type DPI (« Deep Packet Inspection ») très coûteux et ralentissant considérablement le trafic



Mise en œuvre du filtrage (1/2)

- **Aspects juridiques**
  - Nécessité d'assurer la proportionnalité du filtrage par rapport à la liberté d'expression
  - Nécessité d'assurer les droits de la défense
  - Origine de la décision de filtrage : autorité judiciaire ou entité administrative (HADOPI, ARJEL, CSA, ANSSI, DGCCRF, ministères…) ?
- **Aspects techniques**
  - Assurer la gestion de la base de données des filtres
    - Il est facile de créer une liste noire
    - Il est très difficile de la maintenir à jour
      - Exemple : sur 167 sites, seuls 3 auraient dû rester filtrés deux ans après la création d'une liste noire (Suède et Danemark, 2008-2010)
    - Nécessité de procédures bien définies et d'entités administratives en charge de ces procédures
  - Contrôler l'efficacité des mesures au regard de leur coût

Mise en œuvre du filtrage (2/2)

- **Aspects financiers**
  - Coût pour le contribuable des mesures de filtrage
  - Prise en charge par l'État des surcoûts induits par les mesures de filtrage sur les FAI
    - Estimation pour Copwatch : 20-30 équipements DPI + proxy ≈ 12 000 € minimum pour chaque FAI concerné
    - En attente du décret d'application correspondant pour les jeux en ligne
    - Mais les surcoûts liés à la loi « Création et Internet » n'ont toujours pas été remboursés par l'HADOPI…
  - Dommages et intérêts pour les sites bloqués par erreur
  - Coût de gestion administrative de la base des filtres

Inconvénients du filtrage (1/3)

- **Surblocage**
  - Filtrage par l'adresse IP : risque de blocage des sites hébergés sur le même serveur
    - Exemple : un million de blogs bloqués par erreur suite au filtrage de *leakymails.blogspot.com* (Argentine, 2011), blocage mondial de YouTube suite à une erreur de filtrage au Pakistan (2008)
  - Filtrage par le nom de domaine : risque de blocage des sites utilisant le même nom de domaine
    - Exemple : 84 000 sites bloqués par erreur (États-Unis, 2011, sites de type « *ABCD.mooo.com* »
  - Filtrage par l'URL : risque de surblocage lié à l'utilisation d'un proxy
    - Exemple : Wikipédia (Royaume-Uni, 2008)

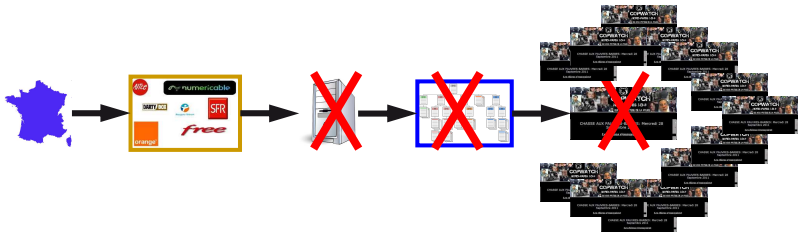
Inconvénients du filtrage (2/3)

- **Portée des mesures de filtrage**
  - Ne concerne que les principaux FAI
    - Copwatch : Bouygues Télécom, Darty Télécom, Free, Numericable, Orange et SFR
    - StanJames.com et 5Dimes.com : idem + Auchan Telecom
  - Choix des FAI concernés effectué par le demandeur ?
  - Pour un total de 1150 opérateurs déclarés à l'ARCEP
    - Égalité devant la loi ?
  - Une obligation de résultat concernant les mesures de filtrage est irréaliste, seule une obligation de moyens est raisonnable
  - Astreintes, dépens : ne pas se tromper de cible !

Inconvénients du filtrage (3/3)

- **« Effet Streisand »**
  - Création de sites miroirs par des internautes suite au buzz médiatique généré

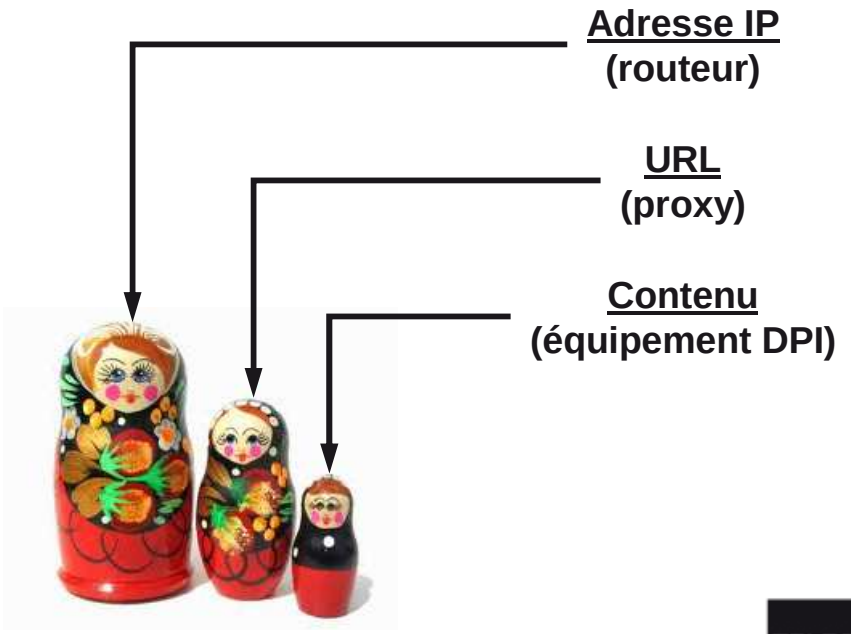
  - Exemples : WikiLeaks (>200), Copwatch (>36)
  - Réaction à des décisions de filtrage perçues comme « injustes » par une partie des internautes
  - Nécessité de « pédagogie » dans les décisions judiciaires ?



Inconvénients du filtrage par DPI

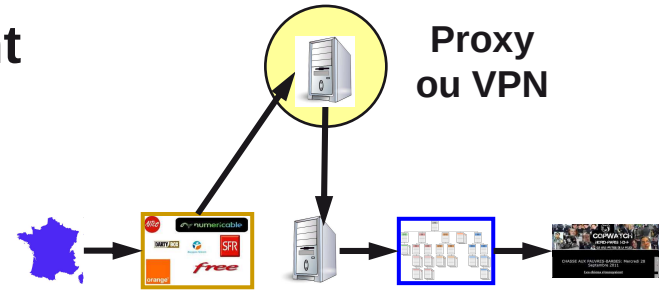
- **Ralentissement du trafic internet**
  - L'inspection du contenu par les équipements DPI induit un ralentissement inévitable du trafic
  - Les équipements DPI sont largement utilisés en entreprise
  - Mais le trafic supporté par un FAI n'a aucune commune mesure avec celui d'une entreprise

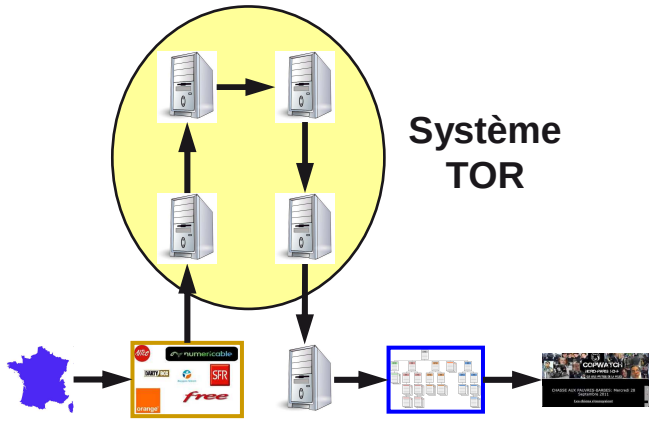
- **Implications en termes de vie privée**
  - L'inspection du contenu pose question concernant le secret des correspondances

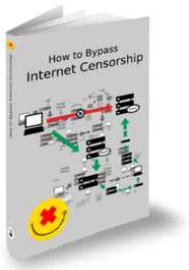


Contournements possibles

- **Proxies web publics, VPN avec chiffrement**
  - Utilisation d'un équipement hors de France (proxy ou routeur VPN)
  - La partie du trafic assurée en France peut être chiffrée pour échapper au filtrage
- **Routage en oignon (TOR)**
  - Utilisation de plusieurs équipements successifs (pelures d'oignon)
  - Le trafic entre chaque équipement est chiffré
- **Usage des contournements**
  - Mise en œuvre simple par des internautes lorsque la motivation est présente
    - Exemple : Tunisie
  - StanJames.com, 5Dimes.com et Copwatch restent accessibles par ces techniques







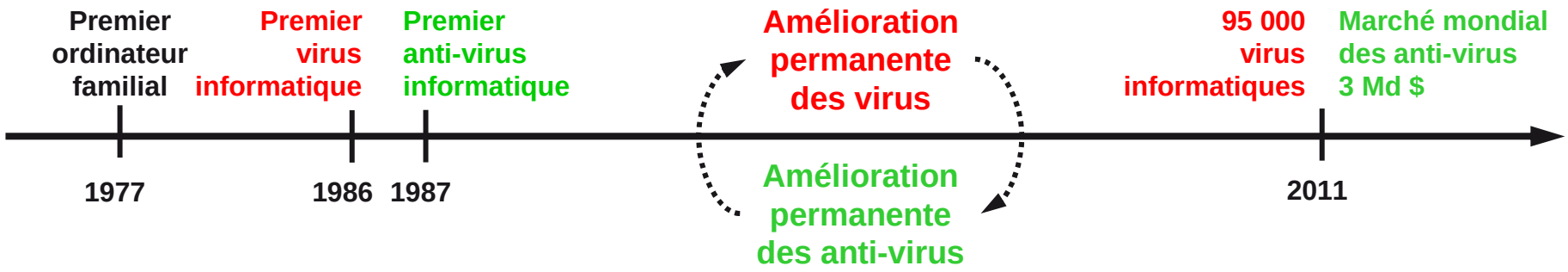
Efficacité du filtrage (1/2)

- **Efficace pour les sites que les internautes ne cherchent pas**
  - Exemples : filtrage de sites pour des raisons de sécurité (spam, virus, phishing), filtrage parental
  - Largement utilisés sur les équipements des internautes (et sous leur contrôle)
- **Peu efficace pour les sites que des internautes cherchent**
  - Existence de nombreux moyens de contournement
  - Les contenus pédopornographiques ne s'échangent pas sur des sites publics !

Filtrer = Interdire l'accès à un site, aux internautes qui de toute façon ne l'auraient jamais visité ?

Efficacité du filtrage (2/2)

- **Pas de gagnant sur le long terme**
  - Exemple : lutte contre les virus informatiques



  - Évolution prévisible des méthodes de contournement en parallèle de celle des techniques de filtrage
  - Le coût du filtrage augmentera avec le temps
  - Il semble plus efficace d'investir sur l'identification des responsables et le retrait des contenus à la source
    - Lutte contre les réseaux mafieux de contrefaçon, etc.

~~Technologies ↔ Technologies~~ Hommes ↔ Hommes

Conclusion (1/2)

- **Le filtrage par les fournisseurs d'accès présente de multiples inconvénients**
  - Coût élevé, efficacité limitée, risque de surblocage et de ralentissement du trafic, non respect de certaines normes techniques (HTTPS, DNSSEC)…
  - Préférer, lorsque c'est possible, les techniques de filtrage les moins intrusives et ayant le moins d'impact sur le trafic et sur le coût (par adresse IP, par nom de domaine)
- **Les actions à la source sont toujours préférables au filtrage**
  - Pour les sites illégaux visant la France : suppression des contenus à la source ou saisie du nom de domaine, ce qui peut nécessiter des accords intergouvernementaux
    - L'internationalisation de la criminalité en ligne impose des liens renforcés entre les juridictions nationales
  - Pour les sites légaux dans d'autres pays : la géolocalisation des visiteurs doit permettre d'interdire l'accès aux internautes français (technique finalement mise en place par StanJames.com)

Conclusion (2/2)

- **Le filtrage doit rester une solution de dernier recours après les actions à la source**
  - Principe de subsidiarité prévu par la LCEN et la loi sur les jeux d'argent et de hasard en ligne
  - Peut-on améliorer les actions à la source en les confiant plus systématiquement à des entités professionnelles, telles que l'OCLCTIC, plutôt qu'aux demandeurs eux-mêmes ?
    - Service « Point de Contact » mis en place en 1998 par les FAI français pour les contenus attentatoires à la dignité humaine
  - Peut-on imaginer des actions préalables de type médiation pour « désamorcer » les cas les moins complexes ?
- **Les solutions choisies doivent en tout état de cause respecter les droits des personnes**
  - Droit à une procédure juste et équitable, droits de la défense
  - Proportionnalité des mesures, respect de la liberté d'expression