

Sujets d'examens

UM1, IPAG, LAP, 2010-2011, Semestre 2

Les sujets sont fournis à titre indicatif et ne sauraient engager l'équipe pédagogique sur un type précis de sujet

partiel
Le semestre

CAP

sujet droit public
donné par M. MAILLOTT

PARTIEL 2^e semestre 2010-2011
IPAG - L.A.P. – Droit public

le 15/2/11
pour le
partiel de
jeudi 17/2/11

Equipe pédagogique : Jean-Marc MAILLOT
Nicolas MARTY
Christophe CANTIE

Dissertation :

L'engagement de la responsabilité de l'Administration

AUCUN DOCUMENT AUTORISE

1^{er} semestre

IPAG

-LAP-

DROIT PUBLIC

SUJET PARTIEL

Du

MARDI 24 MARS 2011

M. Maillot

SUJET :

« Le critère organique dans la définition des contrats administratifs »

Examen
2^e semestre

LAP

- Sujet donné
par M. Naillot
le 7/4/11
pour exam de
lundi 11/4/11
Droit public

IPAG

- LAP -

DROIT PUBLIC

EXAMEN

Du

LUNDI 11 AVRIL 2011

14H - 17H

SUJET :

"Le service public à la française existe-t-il toujours ?"

LAP
Nathapage 2^e semestre

Sujet donné
par M. Maillot
le 26/5/11

Examen 2011
2^{ème} session 2^{ème} semestre
IPAG – L.A.P.
Droit public

JEUDI 9 JUIN 2011 DE 14H A 17H

Equipe pédagogique : M. Jean-Marc MAILLOT
M. Nicolas MARTY
M. Christophe CANTIE

Dissertation :

Les référés soumis à la condition d'urgence.

LAP

EXAMEN 2^e Semestre -

Sujet donné
par M. DELANDE.
le 4/4/11.

LICENCE D'ADMINISTRATION PUBLIQUE

ECONOMIE POLITIQUE

- 12/04/2011 -

14^h → 17^h

Pr. G. DELANDE

A. Répondre sommairement aux questions suivantes (8 pts) :

- 1- Causes et conséquences de la crise de 1975.
- 2- L'approche institutionnaliste en économie.
- 3- Caractéristiques de l'offre compétitive.
- 4- Fonctions de la titrisation.

B. Question rédactionnelle (12pts)

Commentez cette observation de M. D Strauss-Kahn, Directeur du Fonds Monétaire International : « Les conséquences de la crise sont loin d'être épuisées, la situation en Europe reste très préoccupante, l'avenir est plus incertain que jamais ».

naalua faape 2^e demeshe 2010/11

Sujet donné
par Dr Delande
le 27/5/14

LAP
LICENCE D'ADMINISTRATION PUBLIQUE

ECONOMIE POLITIQUE

2^{ème} Semestre – 2^{ème} Session

/2011

Pr. G. DELANDE

Répondre sommairement aux questions suivantes (4 pts par question) :

- 1- Quelles sont les principales caractéristiques du modèle keynésien ?
- 2- Analysez le concept de fluctuations économiques.
- 3- Conséquences de la mondialisation sur les facteurs de production.
- 4- Qu'est-ce qui différencie le chômage classique et le chômage keynésien ?
- 5- Causes de la crise de 2007-2008.

LICENCE D'ADMINISTRATION PUBLIQUE

ECONOMIE POLITIQUE

RATTRAPAGE 2 EME SEMESTRE

08/06/2010

Pr. G. DELANDE

A. Répondre sommairement aux questions suivantes (10 pts) :

1. Quelles sont les principales caractéristiques du modèle néo-classique ?
2. Qu'est-ce qu'un marché dérivé ?
3. Quels facteurs expliquent la croissance exceptionnelle des Trente Glorieuses ?
4. Qu'est-ce qui différencie le chômage classique et le chômage keynésien ?

B. Question rédactionnelle (10pts)

Causes et conséquences de la crise de 2007-2008.

XAMEN

DU

llllllll

2^e semestre

ESPAGNOL

sujet donné par

Pmo. OVILLA



Université Montpellier 1

Instituto de Preparación a la Administración General

CAP ~~de HAD~~

Traduzca el texto siguiente

China muestra su preocupación por el vertido de agua radiactiva al mar en Japón

El Ministerio de Exteriores chino exige a Japón mejor información sobre la crisis nuclear en Fukushima y que asegure la protección del medio ambiente marino

El País JOSÉ REINOSO | Tokio 08/04/2011

El Gobierno chino ha dado hoy la muestra más clara de preocupación en público por la crisis atómica de la planta japonesa de Fukushima desde que comenzó el desastre causado por el terremoto y el tsunami que devastó la costa nororiental de Japón el pasado 11 de marzo. Pekín ha dicho que está inquieto por el vertido de agua radiactiva al mar desde la planta. "Como vecino de Japón, manifestamos de forma natural nuestra preocupación por esto. Esperamos que Japón actúe de acuerdo con las leyes internacionales y adopte medidas efectivas para proteger el medio marino", ha dicho Hong Lei, portavoz del Ministerio de Exteriores, en un comunicado, como informa Reuters. "China está siguiendo de cerca el desarrollo de los acontecimientos, estamos llevando a cabo al mismo tiempo nuestra evaluación especializada, y continuaremos manteniendo un estrecho contacto con Japón. Pedimos a Japón que proporcione la información relevante al lado de chino de forma rápida, completa y precisa".

Fukushima ha estado vertiendo agua radiactiva de forma intencionada al océano para liberar espacio en el que almacenar otra más contaminada. Una parte de la radiación se diluye en el mar, y Tokio ha asegurado que la medida no afectará a la seguridad del pescado en la zona. La central nuclear se encuentra en la costa oriental de Japón, mientras que China está frente a su costa occidental.

La inquietud de Pekín no se debe solo al vertido de agua. Las autoridades chinas han detectado trazas de yodo radiactivo en espinacas cultivadas en la ciudad de Tianjin, la provincia de Henan y la propia capital china, aunque en niveles muy bajos y no dañinos para la salud, según el Gobierno. El Ministerio de Sanidad dijo el miércoles que la contaminación se ha producido por la lluvia caída, que depositó partículas radiactivas en la verdura, y aseguró que basta lavar las hojas de las espinacas para quitar la radiación. Es el primer caso de alimentos producidos en China que han resultado contaminados desde que Pekín ordenó que se realizaran controles a la comida y el agua, debido a la crisis atómica.

Las autoridades chinas han encontrado también radiación en niveles muy bajos en el aire en 22 provincias, y han detectado 10 casos de contaminación radiactiva en pasajeros, aviones, barcos y contenedores procedentes de Japón desde el 16 de marzo.

La fuga de radiación a la atmósfera en Japón ha asustado a muchos chinos, que al inicio de la crisis se lanzaron a comprar sal, en la errónea creencia que el yodo que contiene podría protegerles. El Gobierno japonés ha sido muy criticado por su falta de transparencia tanto dentro como fuera de sus fronteras. Diferentes Gobiernos extranjeros, organizaciones medioambientales y el Organismo Internacional de la Energía Atómica le han pedido que suministre más información, y lo haga con mayor rapidez y claridad.

Traduzca la frase siguiente: (3 puntos)

Par ailleurs la décision, hier, prise par l'Autorité de sureté nucléaire japonaise de relever le niveau de la catastrophe de 5 à 7 est mal comprise par les japonais et les pays voisins. D'autant que dans le même temps le gouvernement annonçait ne plus redouter de fuite importante. De nombreux experts, dont ceux de l'IRSN, estiment que cet accident est de niveau 6 et pas 7. Selon les premières mesures les rejets de matières radioactives à Fukushima représentent 10 % des rejets de Tchernobyl

LAP
Sujet
Examen 2^e semestre.

IPAG

Sujet donné
par M. Valenti
le 6/4/11
pour le Mardi 12/4/11
9h → 12h

- LAP -

HISTOIRE CONTEMPORAINE

EXAMEN

Du

MARDI 12 AVRIL 2011

9H – 12H

Sujet à traiter :

"Les finances pendant l'Etat napoléonien."

LAP

Kallapage 2^e semestre 10/11
deput donnei par Mr.
Valente
le 6/6/11

Examen 2011
2^eme session 2^eme semestre
IPAG – L.A.P.
HISTOIRE CONTEMPORAINE

VENDREDI 10 JUIN 2011 DE 9H A 12H

Equipe pédagogique : M. Fabien VALENTE

Dissertation :

La fonction publique sous la Révolution.

AUCUN DOCUMENT AUTORISE

Nota de Synthèse
partiel du 10/3/09
donné par 91 LESIERC

CAP.

CNS

CONCOURS DE COMMISSAIRE DE POLICE
DES 10, 11 et 12 mars 2009

Epreuve de NOTE DE SYNTHESE et de PROPOSITIONS

Mercredi 11 mars 2009 à 14 heures 30 (heure de Paris)
(durée : 4 heures – coefficient : 4)

—oOo—

SUJET : La cybercriminalité.

A partir du dossier ci-joint consacré à la **cybercriminalité**, rédigez une note de synthèse de **5 pages maximum** et présentez, dans une conclusion d'une quinzaine de lignes maximum, votre opinion sur la question.

Document n°1 (pages 2 à 8) : *Les nouvelles menaces criminelles numériques* - Cahiers de la sécurité (octobre-décembre 2008) - Laurence Ifrah.

Document n°2 (pages 9 à 19) : *Les technologies numériques du futur : nouvelles menaces, nouvelles vulnérabilités* - Cahiers de la sécurité (octobre-décembre 2008) - Michel Riguidel.

Document n°3 (pages 20 à 23) : *Cybercriminalité* - Enjeux de mots : regards multiculturels sur les sociétés de l'information - 5 novembre 2005 - Alain Ambrosi, Valérie Peugeot et Daniel Pimienta.

Document n°4 (pages 24 à 26) : *Un monde numérique particulièrement vulnérable à la criminalité* - Problèmes politiques et sociaux : la délinquance électronique - octobre 2008 - Solange Ghernaouti-Hélie.

Document n°5 (page 27) : *Les différentes facettes du cyberspace criminologique* - Problèmes politiques et sociaux : la délinquance électronique - octobre 2008 - Stéphane Leman-Langlois et Marc Ouimet.

Document n°6 (page 28) : *L'évolution des cybercrimes : données 2004* - Problèmes politiques et sociaux : la délinquance électronique - octobre 2008 - Conseil de l'Europe.

Document n°7 (page 29 à 34) : *L'arsenal juridique français* - Problèmes politiques et sociaux : la délinquance électronique - octobre 2008 - Myriam Quémener.

Document n°8 (page 35 à 38) : *La coordination de la lutte contre la cybercriminalité dans l'Union européenne* - Problèmes politiques et sociaux : la délinquance électronique - octobre 2008 - Commission des communautés européennes.

Document n°9 (page 39 à 41) : *Un nouveau défi pour les systèmes de justice pénale* - Problèmes politiques et sociaux : la délinquance électronique - octobre 2008 - Conseil de l'Europe.

N.B. : Les candidats s'assureront être en possession de l'intégralité des documents (41 pages numérotées de 1/41 à 41/41) et de la qualité de leur impression dès le début de l'épreuve.

DOCUMENT N°1

Les nouvelles menaces criminelles numériques

Laurence IFRAH



La menace numérique n'a jamais été si préoccupante. Aujourd'hui, les médias communiquent régulièrement sur ce fléau et les utilisateurs sont beaucoup mieux informés des risques qu'ils encourent à surfer sur la toile. Pourtant, les organisations criminelles qui opèrent sur Internet n'ont jamais été aussi puissantes. Elles ne visent plus seulement l'ensemble des internautes, mais des utilisateurs ciblés selon un profilage précis du type de victime auquel correspond une forme d'attaque spécifique.

The New Threats of Electronic Crime

The threat of electronic crime has never been so preoccupying. Today's media regularly communicate to the public the nature of this scourge and citizens are much better informed of the risks they run when surfing on the net. Nevertheless, the criminal organisations that operate on the net have never been so powerful. They no longer target all users, but now aim at particular categories of the population that have been carefully profiled as vulnerable victims.

Laurence Ifrah
Criminologue spécialisée en criminalité numérique au Département de recherches sur les menaces criminelles contemporaines (DRMCC) de l'Institut de criminologie de Paris, Université Paris II Panthéon-Assas, consultant en sécurité des systèmes d'information, expert en recouvrement de données et en analyse de supports numériques. Elle a été auditeur de la 19^e session nationale de l'INHES. Elle intervient auprès des étudiants de 3^e cycle du DRMCC sur la criminalité numérique et auprès de l'Institut d'études judiciaires.

La communauté internationale commence enfin à prendre conscience de l'urgence à mettre en place des moyens de protection contre le cybercrime. Des pays comme les États-Unis et l'Estonie ont mis en œuvre des structures offensives et défensives capables d'analyser et de répliquer à de nombreuses formes d'attaques, après avoir subi des offensives répétées et parfois massives. Les moyens utilisés seront forcément les mêmes d'un côté comme de l'autre, ce qui implique que les éditeurs d'antivirus devront éviter de reconnaître certaines signatures de « malwares » pour permettre aux États d'infiltrer à distance des ordinateurs ciblés. Il ne reste qu'à espérer que les organisations criminelles ne profitent pas de cette aubaine pour mieux développer leurs activités car leurs moyens budgétaires sont bien souvent supérieurs à ceux des administrations, au quotidien en tout cas.

La progression du crime numérique

Quelques faits récents

Voici quelques faits récents qui démontrent l'inquiétante progression du crime numérique en 2008, tant au niveau de la technologie qu'au niveau des vecteurs de diffusion.

Avril 2008

L'achat de périphériques de stockage de données devient risqué, et il est désormais préférable de passer un antivirus et de formater le matériel avant de l'utiliser. Des disques durs et des clés USB ont été altérés pendant leur production en Chine et diffusés sur le marché occidental à l'insu des marques et des distributeurs. Fait nouveau depuis novembre 2007, des éditeurs d'antivirus ont constaté la présence de chevaux de Troie sur des disques durs et des clés USB neufs. Après enquête, il s'est avéré que les infections de ces matériels avaient eu lieu sur les sites de production dans des usines basées en Chine. L'éditeur Kaspersky a été le premier à faire état du problème sur les disques durs Maxtor de Seagate qui contenaient un cheval de Troie chargé, entre autres, de désactiver et de récupérer les mots de passe des joueurs en ligne pour les expédier sur un serveur basé en Chine et de désactiver les antivirus. L'entreprise a confirmé la situation sur son site Web et fait immédiatement rappeler 3 600 disques durs de 500 Go.

...

(1) www.viruslist.com

(2) Le Better Business Bureau est un conseil d'éthique commercial chargé des relations entre les entreprises et les consommateurs. Il est présent aux États-Unis et au Canada dans plus de 140 villes.

(3) www.f-secure.com

Puis, c'est au tour de Hewlett-Packard, en Australie, d'apprendre que des clés USB de 256 Mo et de 1 Go offertes à ses nouveaux clients (acheteurs d'imprimantes) avaient également été corrompues, à leur insu, par un code malveillant. En janvier, c'était l'importateur hollandais qui proposait à la vente des lecteurs médias de la marque Victory LT-200, également fabriqués en Chine. Ces périphériques propageaient un ver sur les machines connectées à un réseau de partage de fichiers¹.

Mai 2008

Les moyens de compromission des ordinateurs sont plus sophistiqués et il devient difficile de différencier la mise à jour d'un produit licite de celle d'un code malicieux. L'affichage est identique et paraît le plus souvent légitime. En mai 2008, plus d'un demi-million de pages Web ont été compromises par Zlob Trojan (figure 1), un cheval de Troie déguisé en décodeur vidéo. Les internautes étaient invités à télécharger un utilitaire pour visualiser les vidéos proposées sur les sites Internet. En cliquant dans la fenêtre affichée, ils installaient le malware qui permettait au pirate de prendre le contrôle à distance de leur ordinateur.

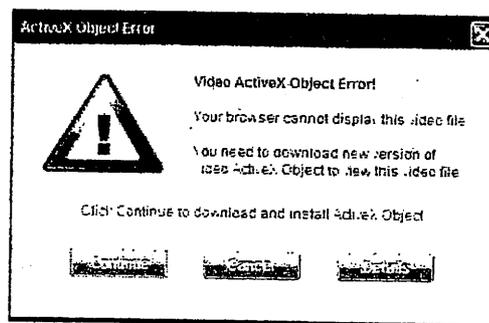


Figure 1 - Zlob Trojan

Les nouvelles versions de « spams » infectés par des chevaux de Troie ne sont plus envoyées en masse à n'importe quel destinataire, ils sont à présent conçus pour des victimes préalablement sélectionnées en fonction de leur activité dans l'entreprise qui les emploie. Des cadres supérieurs de très grands groupes américains ont été visés par un e-mail frauduleux prétendant émaner du Better Business Bureau² aux États-Unis, et qui ouvre les systèmes d'information de leur entreprise aux pirates³. L'e-mail précisait le nom du destinataire, sa fonction et les coordonnées de la société qui l'employait. Le texte indiquait

qu'une plainte avait été déposée à l'encontre de son entreprise et l'invitait à télécharger le document en cliquant sur un lien qui demandait de télécharger une mise à jour du logiciel Acrobat de l'éditeur Adobe ainsi qu'un contrôle ActiveX. Ce dernier, une fois installé, ouvrait une « backdoor »⁴ qui donnait accès au système d'information et permettait de collecter des données personnelles et confidentielles. Autre détail, le lien dirigeait l'internaute vers le site www.us-bbb.com alors que l'adresse véritable du Better Business Bureau est www.us-bbb.org (figure 2).

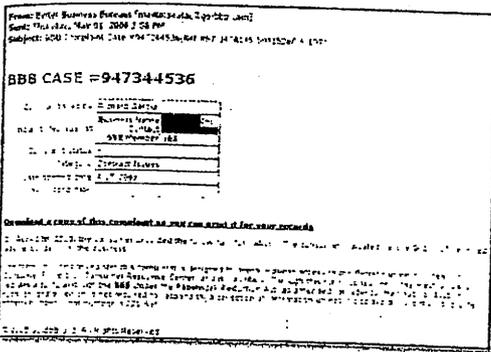


Figure 2 - e-mail frauduleux ciblé

Autre exemple, un pirate chilien a publié sur deux sites internet les informations personnelles de six millions de ses compatriotes après les avoir récupérées sur des bases de données du gouvernement. Ces données comportaient entre autres, les noms, prénoms, adresses et numéros de téléphone des victimes⁵.

Juin 2008

Un gang de pirates exploite actuellement les événements de l'actualité internationale en diffusant de faux flashs d'information via des spams infectés⁶. L'éditeur d'anti-virus Sophos a intercepté des e-mails dont les titres sont liés à la présence des forces armées américaines au Moyen-Orient :

- la troisième guerre mondiale a débuté ;
- 20 000 soldats américains en Iran ;
- l'armée américaine a franchi la frontière iranienne.

Juillet 2008

Une faille DNS⁷ découverte en début d'année par Dan Kaminsky, expert en sécurité des systèmes d'information chez IOActive, aurait pu être à l'origine d'un véritable désastre économique sur Internet. Les serveurs DNS assurent la correspondance entre un nom de domaine (par exemple : www.google.fr) et son adresse IP (209.85.135.99), un système mis au point pour simplifier la saisie des adresses d'un site Internet car il est plus facile de se souvenir de www.google.fr que de 209.85.135.99. Les serveurs DNS disposent de caches pour garder en mémoire les adresses saisies par les internautes, ceci permet de diriger l'utilisateur directement sur le site de son choix en réduisant le temps d'attente et sans avoir à solliciter constamment les autres serveurs DNS. La faille décelée (aussi connue depuis 2004⁸ sous le nom de DNS « pharming » ou encore de DNS cache « poisoning ») permet à un pirate de modifier ces caches à distance pour rediriger les internautes sur des sites de « phishing ». Ces derniers, alors convaincus d'être sur des sites légitimes, communiquent sans hésitation leurs informations personnelles.

Ce sont là quelques-uns des faits marquants de l'année 2008. Dans la société de l'information, le vrai danger c'est ce que l'on n'a pas vu, pas su ou pas pu voir. Nous ne reprendrons pas ici les poncifs et sempiternels exemples ressassés partout, mais ce qui se passe vraiment aujourd'hui, en 2008, avec pour perspectives les nouvelles menaces informatiques, celles qui seront dominantes et qui émergent aujourd'hui.

L'explosion des malwares⁹

Le premier million de malwares (dont 60 % de chevaux de Troie), en circulation sur Internet, sera atteint et même largement dépassé au courant du deuxième semestre 2008, soit plus du double depuis le début de l'année. Quelle que soit la technique employée pour permettre la diffusion de ces codes malicieux, il n'existe que deux moyens de les transmettre sur un ordinateur :

- la vulnérabilité système ou applicative ;
- le « Social Engineering »¹⁰.

DOSSIER

 (4) Porte dérobée.
 (5) www.TheRegister.co.uk
 (6) Sophos antiVirus.
 (7) Domain Name System.
 (8) www.idg.net
 (9) Contraction des mots *malicious* (pour code malicieux) et *software* (pour logiciel).
 (10) L'art de la manipulation de personnes tierces, souvent crédules, qui représentent le point central d'une attaque afin d'obtenir des informations confidentielles permettant d'accéder à des ressources protégées.

La vulnérabilité système ou applicative

La vulnérabilité système est toutefois moins exploitée que l'applicative ; le « Drive-by download » est une technique qui utilise les failles présentes dans les logiciels tels que les navigateurs Internet pour y insérer des codes malveillants qui s'installent automatiquement et en toute transparence sur les ordinateurs des internautes, sans intervention de leur part. Pour infecter le plus d'internautes possible, les pirates injectent du code malveillant (JavaScript) sur les pages des sites web les plus populaires comme les moteurs de recherche ou les magazines en ligne. Les éditeurs s'efforcent de publier des mises à jour correctives dans les meilleurs délais pendant que les organisations criminelles offrent des sommes allant jusqu'à 75 000 dollars pour obtenir l'information et l'exploiter le plus longtemps possible.

Le Social Engineering

Le social engineering, utilisé depuis des années, prend aujourd'hui une tournure plus perfide. Ce mode opératoire, particulièrement prisé par les organisations criminelles (majoritairement situées en Russie, en Ukraine, en Roumanie et dans d'autres pays d'Europe de l'Est), est utilisé pour installer des codes malveillants destinés à leur permettre de prendre le contrôle à distance des ordinateurs

des utilisateurs. Le professionnalisme dont ces organisations font preuve se remarque dans cette formidable capacité à tromper l'utilisateur et à améliorer en permanence les techniques d'approche, en réalisant un ciblage précis de leurs futures victimes grâce à des leurreurs de plus en plus sophistiqués. Ainsi, de nombreux e-mails ont été envoyés à des cadres supérieurs dans des entreprises. Les messages indiquent précisément le nom, le poste de la victime et celui de sa société. Ils émanent d'organismes d'État comme le FBI, le fisc ou la Cour de Justice et semblent parfaitement crédibles (figure 3).

Des attaques politiques

Les attaques motivées par l'actualité politique sont également en nette progression. Lors du conflit récent entre les militaires chinois et les Tibétains, de nombreux e-mails piégés ont envahi les forums des organisations humanitaires qui soutenaient « la libération » du Tibet. Les internautes, soigneusement ciblés en fonction de l'importance de leur soutien aux « rebelles », recevaient des e-mails au contenu parfois illustré par des photos de Tibétains malmenés par des militaires chinois. Ces e-mails semblaient être expédiés par des personnes de confiance, parfaitement connues des destinataires (figure 4). Les chevaux de Troie présents dans les fichiers joints aux formats standards des logiciels de bureautique permettaient à ses expéditeurs d'espionner les ordinateurs de leurs victimes à leur insu. Selon F-Secure, des malwares similaires ont été repérés dans des attaques contre des entreprises ce qui porterait à croire que les auteurs de ces codes offensifs seraient motivés par des raisons politiques mais également intéressés par les activités de l'industrie liée au secteur de la Défense.

50 % des attaques sont réalisées pour des motifs idéologiques. Les partis politiques, leurs candidats et certains départements d'États subissent régulièrement des défacements de leurs sites Web sur lesquels les opposants laissent des messages de propagande. On note une hausse sensible de ces défacements à l'approche d'élections.

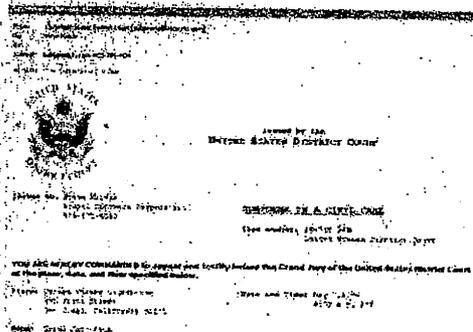


Figure 3

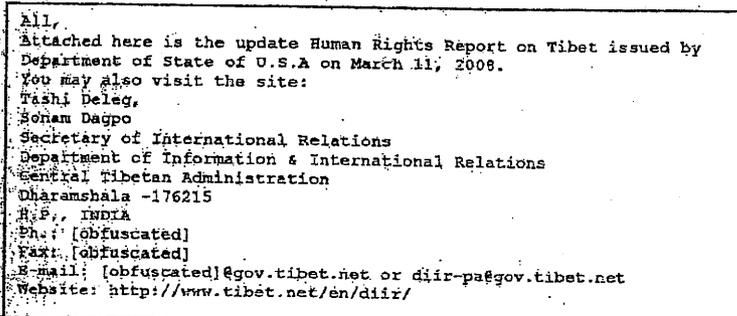


Figure 4 - E-mail piégé

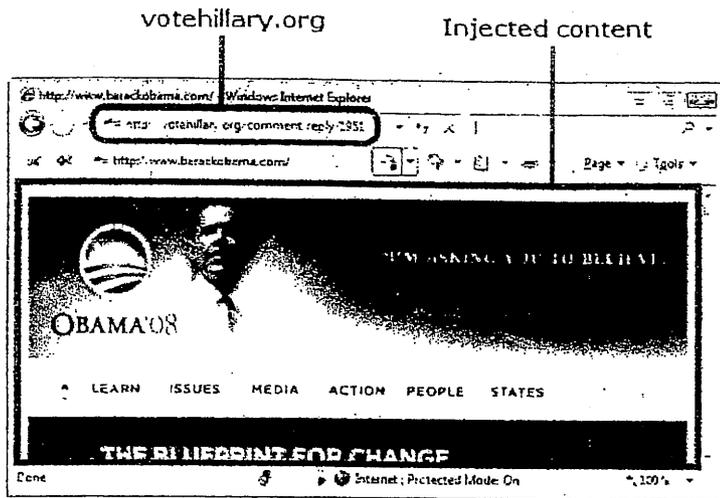


Figure 5 - Redirection du site d'Obama vers celui de Clinton
Source : www.barackobama.com

En avril 2008, le site de Barack Obama a été attaqué par une injection de code qui lors de la saisie de l'URL de son site web, redirigeait les internautes vers celui de sa rivale Hillary Clinton (figure 5).

Les nouveaux « Botnets »

À l'origine de la diffusion de tous ces maux, se trouve une technique d'attaques massives, les botnets. Jusqu'en 2006, on pouvait détruire un botnet en supprimant le poste de contrôle et de commande du pirate que l'on tentait de retrouver plus ou moins aisément. Aujourd'hui, et ce depuis l'apparition au début de l'année 2007, d'une nouvelle forme de Botnet dont Storm Worm (conçu par la tristement célèbre organisation criminelle RBN¹¹), qui se propage sur les réseaux Pair-à-pair (Peer2Peer), il est impossible de localiser ce poste de commande. Entre juin et juillet 2007, 1 700 000 machines étaient infectées contre 2 817 entre mai et juin 2007. 71 342 attaques ont pu être bloquées les cinq premiers mois de 2007 ; elles sont passées à plus de 20 millions entre juin et juillet¹². Le 24 juillet 2007, sur 46,2 millions de spams détectés, plus de 99 % contenaient le ver Storm¹³.

Technique et stratégie

Le système pair-à-pair permet de nommer un ensemble constitué d'utilisateurs (en nombre pas forcément défini, ni fixe, mais plutôt de manière générale), du protocole qui leur permet de communiquer (Gnutella, BitTorrent, CAN, etc.), et du fonctionnement du protocole entre ces machines. Le terme de « réseau pair-à-pair » permet de désigner les machines et leur interconnexion à un moment donné, avec un nombre défini de machines/utilisateurs.

Dans un système pair-à-pair, les postes utilisateurs ne jouent pas exclusivement les rôles de client ou de serveur mais peuvent assurer parallèlement les deux fonctions. Ils sont en effet simultanément clients et serveurs et jouent aussi le rôle de routeur, en passant les messages de recherche, voire les données vers leurs destinataires. Cette architecture réseau permet ainsi aux Botnets de se déployer, sans qu'il soit possible de localiser le poste de contrôle et de commande principale, chaque ordinateur infecté étant un porteur du virus indépendant, si un poste est supprimé, un autre prend immédiatement la relève. À ce jour, il n'a pas été possible de quantifier précisément le nombre de PCs compromis par Storm, mais on a évalué le Botnet à environ 20 millions de machines, au plus fort de sa

DOSSIER

(11) Le Russian Business Network est aussi l'auteur de nombreux logiciels offensifs dont MPack qui a été mis à disposition dans une version commercialisée à 700 dollars l'unité, sur les forums russophones lors des attaques contre l'Estonie, en avril 2007.

(12) SecureWorks.

(13) Cf. Postini, spécialiste de la messagerie hébergée sécurisée.

performance. Aucune parade n'a été mise en place, et les experts en sécurité des systèmes d'information affirment qu'aucune forme de protection disponible actuellement ne pourrait stopper une attaque de déni de service lancée par Storm. Un groupe de chercheur finlandais a cependant tenté de tuer le vers en infectant le code malveillant, une tentative réussie temporairement car une des particularités de Storm est sa capacité à mettre à jour ses propres failles en quelques heures. Storm est le premier botnet intelligent, il sait sélectionner les ordinateurs bénéficiant du haut débit pour diffuser ses spams infectés afin d'agrandir son réseau, soit environ 30 000 à 40 000 spams par heure et par ordinateur zombie. Outre l'envoi de spams, il est utilisé pour diverses formes d'attaques, le phishing, le Ddos (Déni de service distribué), les attaques sur messageries instantanées, etc. Storm est également pourvu de capacité de défense et s'attaque violemment aux organisations spécialisées dans la lutte contre les botnets en activant son réseau de PCs zombies pour lancer des connexions simultanées - par centaines de milliers - sur leurs serveurs, afin de les rendre indisponibles.

Mais rappelons-le, le spam n'est que la partie visible de l'iceberg, les botnets ont beaucoup de ressources et sont générateurs de revenus substantiels, parmi les nombreuses activités, les plus courantes sont :

- le « Pump and Dump » ;
- la vente de produits illicites en ligne ;
- le chantage, la menace et l'extorsion (casinos et *book-makers*) ;
- l'installation à distance d'outils offensifs (« Keyloggers ») ;
- la collecte d'informations personnelles (fraude bancaire et identitaire) ;
- la corruption de réseaux sensibles pour accéder à des données confidentielles (espionnage industriel) ;
- les attaques de Ddos (Déni de service distribué, dans le cas de l'Estonie ou des entreprises spécialisées dans la lutte contre le crime numérique).

Le Pump and Dump est une escroquerie bien connue des marchés boursiers qui consiste à gonfler artificiellement le cours d'une entreprise avant de vendre d'un coup toutes les actions dont le détenteur majoritaire dispose, et de la mettre généralement en faillite. Grâce à son réseau d'ordinateurs zombies, Storm a diffusé des millions de spams aux internautes pour les inciter à acheter des actions de sociétés sélectionnées pour ce type d'opération. Des prix attractifs et une bonne communication semblaient

rendre l'affaire prometteuse. Les futures victimes ont fait monter le cours de l'action jusqu'au jour où les malfaiteurs ont vendu en masse et se sont retirés en empochant une plus value conséquente. Ainsi, le 7 août 2007, Sophos, éditeur d'antivirus, a détecté plus de 500 millions d'e-mails conseillant aux internautes d'investir dans la société Prime Time Stores Inc., domiciliée à Puerto Rico. Cette campagne a généré, en 24 heures, une hausse spectaculaire de 30 % du nombre de spams dans le monde.

Storm est, entre autres, utilisé pour promouvoir la vente de médicaments en ligne via des pharmacies virtuelles qui délivrent au client des produits de contrefaçon originaires de Russie et d'Inde. Selon IronPort¹⁴, filiale de Cisco, ces revenus seraient dédiés au développement du Botnet et d'autres malwares. Pour éviter la localisation de ces sites illicites, Storm utilise les techniques de fast-flux DNS qui permettent d'attribuer des milliers d'adresses IP à un même nom de domaine. Le système fonctionne de la façon suivante. Un individu possède un site dont le nom de domaine est, imaginons, www.pharmacie.com. Pour que les internautes puissent s'y connecter, il faudra leur attribuer une adresse IP, par exemple 80.246.10.132. Il est possible de bloquer cette IP pour que personne ne puisse s'y connecter. Pour éviter de se faire repérer, les malfaiteurs utilisent une technique parfaitement légale de répartition de charge de serveurs DNS afin d'empêcher une saturation en cas de connexions multiples. À la seule différence qu'au lieu d'effectuer cette répartition de charge sur des serveurs DNS, ils vont utiliser leurs Botnets et les milliers d'ordinateurs infectés pour attribuer autant d'adresses IP à leur nom de domaine. Ces IP seront alors celles des ordinateurs compromis des utilisateurs qui ignorent totalement l'activité se déroulant sur leurs machines. Cela permet ainsi de changer l'adresse IP toutes les trois minutes, une fois l'IP du site sera localisée en France, une autre fois en Suède ou en Chine. Le Fast-Flux DNS est une technique qui évite aux malfaiteurs de se faire localiser et leur offre une redondance optimale.

Storm est extraordinairement créatif en matière de Social Engineering, son vecteur d'infection favori. Depuis sa création, il a diffusé des dizaines de versions de spams infectés sur des thèmes continuellement adaptés à l'actualité, aux événements sportifs, aux fêtes de Noël, du jour de l'An, de la Saint-Valentin et même à la sécurité informatique, en promouvant la vente de logiciels « antispyware » qui, bien-sûr, étaient chargés de corrompre les ordinateurs des internautes crédules.

....

(14) *Special Report - 2008 Internet malwares trends.*

Depuis, cette technique a fait des émules et les malfaiteurs s'en sont inspirés pour créer des botnets, toujours plus performants et plus malveillants. Bobax, Kraken, Mayday et Mega-D sont les nouvelles versions en circulation sur la toile. Kraken aurait infecté en avril 2008, cinquante des entreprises du Fortune 500 et serait indétectable par plus de 80 % des antivirus¹⁵.

Quelques réflexions prospectives

Il s'agit désormais de prendre conscience de l'étendue des compétences de très haut niveau dont disposent les organisations criminelles. Il n'y a pas « seulement » l'aspect technique informatique, mais un ensemble de professionnels issus de la finance, du domaine juridique, du marketing et de la communication et, dans certains cas, (médicaments, stupéfiants et autres produits illicites) de la logistique. Plus récemment, on note la présence de traducteurs et de rédacteurs (souvent des « correspondants locaux »), chargés de rédiger des textes convaincants dans la langue du pays ciblé (rarement le même que celui d'où l'attaque est originaire), ces derniers sont parfois des

acteurs de l'intelligence économique, experts dans l'art de la manipulation.

Ces nouvelles tendances prennent des proportions alarmantes, d'autant plus que les internautes mieux informés sur les risques qu'ils encourent notamment par e-mail, se fient à des points de reconnaissance qui leur ont été répétés depuis des années, à savoir n'ouvrir qu'un e-mail qui provient d'une personne connue, qui leur est adressé nominativement et dont le sujet les concerne. Des éléments qui ne correspondent désormais plus à la réalité.

Les États seront amenés à court terme à créer des cellules réunissant les mêmes compétences, c'est-à-dire des experts du blanchiment d'argent et de la finance, de l'intelligence économique, de la géopolitique, de la logistique, du trafic de stupéfiants et de la contrefaçon, du terrorisme, de l'énergie, des stratèges (militaires), des criminologues et des avocats pour lutter efficacement contre l'envahissement de la toile par les malfaiteurs qu'ils soient criminels, terroristes ou hacktivistes. S'en tenir exclusivement aux aspects techniques serait une coûteuse erreur.

Laurence IFRAH

(15) <http://www.darkreading.com>;

DOCUMENT N°2

Les technologies numériques du futur : *Nouvelles menaces, nouvelles vulnérabilités*

Michel RIGUIDEL



Doit-on craindre un Hiroshima numérique, une future guerre impitoyable des réseaux ? Doit-on redouter un Tchernobyl numérique où des apprentis sorciers provoqueraient une panne cataclysmique ? Peut-on imaginer la conjugaison d'attaques et de pannes entremêlées ? Cet article présente un état des lieux, analyse les menaces et les vulnérabilités futures, remet en question quelques dogmes en sécurité numérique et ouvre des perspectives de recherche.

The Digital Technologies of the Future: New Threats and Vulnerabilities

Should we fear a digital Hiroshima, an unsparing network war? Should we be wary of a digital Chernobyl where any sorcerer's apprentice may provoke a cataclysmic breakdown? Is it possible to imagine a combined attack and breakdown? It is important to analyze our current situation, future threats and vulnerabilities so as to call into question some of our security dogmas in order to open new perspectives and fields of research.



Michel Riguidel est chef du département Informatique et Réseaux à Télécom ParisTech, anciennement, École nationale supérieure des télécommunications. Il enseigne la sécurité et les réseaux avancés. Il consacre sa recherche à la sécurité des réseaux du futur, avec un engagement fort dans la Communauté européenne. Il a publié *Le téléphone du futur* (Pommier, 2004), dirigé la publication *La sécurité à l'ère numérique* (Hermès, 2004) et le chapitre sur la sécurité des systèmes et des réseaux de *L'encyclopédie informatique et des systèmes d'information* (Vuibert, 2006).

La fragilité du Village virtuel violent

Le cyberspace : deux gros nuages enchevêtrés

La dépendance de l'humanité envers les fragiles édifices numériques est devenue inquiétante. Les édifices numériques sont Internet et le Web, les réseaux de télécoms, de diffusion de télévision, de constellations satellites, les systèmes d'information des entreprises, des administrations et des institutions, les systèmes informatiques critiques de contrôle des infrastructures nucléaires, électriques, routières, hospitalières, logistiques, les systèmes de contrôle-commande (alarme, climatisation des immeubles, électronique des voitures), les réseaux WiFi à la maison.

Le Village virtuel violent des citoyens et des entreprises constitue un halo intangible, une enveloppe composée de deux nuages intriqués : le nuage actif dispersé des programmes informatiques de plus en plus opaques, mobiles et devenus incontrôlables, et le nuage passif éparpillé des informations volatiles ou persistantes. Ce cyberspace s'est réincarné en une vulnérabilité béante dans nos sociétés développées, ouvert à tous les vents agressifs ou subversifs, dans lesquels peuvent s'immiscer et se dissimuler ceux qui vivent en marge des lois de nos sociétés, et ceux qui combattent les valeurs de nos civilisations. Le danger majeur de ce règne numérique, récemment installé aux côtés des règnes animal, végétal et minéral, dans sa complexité inextricable et dans son usage critique, résulte essentiellement, pour son volet technique, de la faiblesse architectonique des infrastructures, de l'obscurcissement du nuage des logiciels d'une part, et de l'expansion envahissante du nuage des données disséminées, d'autre part.

En effet, les logiciels sont de plus en plus obscurs : secret de fabrication oblige, cette éclipse partielle marque l'échec du mouvement des logiciels libres qui rêvait d'un monde dématérialisé, ouvert et transparent. Par ailleurs, dans un univers de compétition, la valeur d'un pays se mesure, entre autres, par la valeur de ses biens intangibles : droits de propriété intellectuelle, logiciels, bibliothèques, musées, contenus vidéo et cinéma, organisations numérisées. Enfin, le volume des données double chaque année, croissance encouragée par la baisse du prix des

supports de stockage qui diminue dans ce même rapport. Chaque individu possède en moyenne un patrimoine de dizaines de gigaoctets, masse considérable de logiciels boursoufflés, d'informations fongibles, surabondantes, magma de bits pléthoriques quand on le compare aux quelques centaines de mégoctets qui suffisent à conserver toute l'œuvre de Jean Sébastien Bach, de Victor Hugo ou aux quelques téraoctets pour mémoriser tout le cinéma muet ! [Riguidel, 2006, p. 83].

L'usage numérique en évolution rapide

La résistance des infrastructures numériques a dû se renforcer ces dernières années pour faire face aux sollicitations croissantes d'échanges massifs en temps réel. Leur seuil de tolérance aux pannes et aux attaques a augmenté lorsque l'on considère les variations sévères de flux, l'immédiateté des requêtes d'internautes, l'impatience des adeptes de SMS ou du téléphone mobile, l'addiction des adolescents envers des applications ludiques multijoueurs. La technologie numérique soutient les infrastructures vitales, supporte l'urgence d'une alarme, étaye la défense d'un pays. Cette clef de voûte façonne aussi le divertissement et contribue à l'ampleur de la société du contact et du spectacle.

L'usage numérique s'est profondément modifié du côté des citoyens et des entreprises : la messagerie, l'affichage, la recherche d'informations sur le Web ont été supplantés par le commerce électronique, par des services plus appropriés, avec des objectifs de performance et d'instantanéité, une exigence d'urgence au détriment de la réflexion, de la vraie communication et d'une vision à long terme. Le dimensionnement de ces infrastructures anticipe, avec une avance de quelque dix-huit mois seulement, la lente et sûre progression des ressources informatiques, ce qui permet d'absorber toutes les requêtes des utilisateurs : ressources de trafic sur les réseaux optiques, de bande passante radio, de stockage des serveurs et de puissance de calcul. Mais le paysage informatique, autrefois filet diffus de routes et de serveurs informatiques, se modifie en autoroutes pratiquement congestionnées, en centres stratégiques d'aiguillages (comme le *Global Internet eXchange*, nœuds d'interconnexion de réseaux d'Amsterdam), en pôles archi-concentrés de serveurs (comme le site de Google). Les flux gigantesques (100 Gigabits/s) de données entre Systèmes autonomes fusionnent et se concentrent : une congestion de ces infrastructures est à craindre ¹.

DOSSIER

(1) Le 24 février 2008, le site web YouTube a été inaccessible, suite à une action délibérée venant du Pakistan, par un détournement d'adresse IP sur le protocole BGP (Border Gateway Protocol), le protocole de l'Internet pour les interconnexions entre opérateurs, à cause de vidéos blasphématoires.

En outre, le Web, tissu déchiqueté d'utilisateurs novices, constitue un monde angélique de coopération, les protocoles de communication étant aujourd'hui employés loyalement. Mais, si un nombre significatif, pas forcément élevé, d'utilisateurs détournait la fonction normale des logiciels de base et des protocoles en téléchargeant et installant un ersatz malveillant à partir du Web, rien ne fonctionnerait plus².

La responsabilité excessive des utilisateurs otages

Le patrimoine numérique, entrelacs d'infosphères

Chaque bit du cyberspace est la propriété³ d'une personne physique ou morale. L'ensemble des bits (données et logiciels) dont on est possesseur, constitue l'infosphère personnelle [Riguidel, 2004]. Ce peut être l'infosphère d'un utilisateur standard (ses données personnelles sous son contrôle, ses données hors de sa portée dans les bases de données de ses fournisseurs, les traces de géolocalisation chez son opérateur de télécoms), mais ce peut être aussi l'infosphère d'un éditeur de logiciel, laquelle s'étend sur des millions d'ordinateurs d'utilisateurs.

Chaque bit du cyberspace est utilisé par un usager principal. L'ensemble des bits (données et logiciels) que l'on utilise, constitue le patrimoine numérique personnel. L'usager est aujourd'hui responsable de son patrimoine. Ce patrimoine, en général, ne lui appartient pas, car l'usager final utilise de nombreux logiciels, dont il n'est pas propriétaire, mais dont il acquiert seulement la licence d'utilisation. Les deux notions de patrimoine et d'infosphère s'entrecroisent puisque chaque utilisateur exploite de nombreux fragments d'infosphères qui appartiennent à de multiples propriétaires. L'usager standard est de plus en plus prisonnier des logiciels qu'il utilise. Sa vie privée est menacée, car il possède une infosphère personnelle visible par les infosphères opaques des propriétaires de logiciels qui recueillent des données directes ou indirectes, à son insu. Et pourtant, quand l'usager commet une erreur sur son patrimoine, il est le seul responsable.

La souveraineté perdue de l'infosphère personnelle

La souveraineté numérique du cyberspace est mise à mal, ce qui soulève une inquiétude majeure dans nos sociétés démocratiques fondées sur la responsabilité des personnes physiques ou morales. Les usagers, qui sont responsables des actions et des préjudices provoqués par l'utilisation des logiciels dont ils ont payé la licence, ne contrôlent plus l'exécution de ces logiciels. Un ordinateur personnel, sous la responsabilité de son utilisateur, exécute des centaines de processus que le novice, ou même l'expert, ne maîtrise absolument plus, comme la mise à jour des applications, des antivirus, du système d'exploitation. On lui demande seulement de cliquer ! L'usager responsable maîtrise de plus en plus mal son patrimoine numérique, modifié en temps réel et en flux tendus par les différents propriétaires, sans que le gestionnaire de ce patrimoine soit réellement informé.

La dignité évincée de l'infosphère personnelle

La dignité numérique [Riguidel, 2006, p. 521] des usagers responsables risque d'être bafouée si on ne réagit pas rapidement, en émettant des règles dans le monde virtuel, règles similaires aux principes du monde réel, et en renouvelant les outils de prévention et de régulation de l'écosystème. Les utilisateurs sensibilisés (personnes ou entreprises) savent protéger la partie de leur infosphère privée, engendrée de leur plein gré et sous leur contrôle. En revanche, la partie de l'infosphère intime des individus et des entreprises, qui est hors de leur portée et enregistrée à leur insu, leur échappe totalement. Toute leur vie privée est fragilisée par une intrusion potentielle de leur infosphère, en dehors de leur contrôle et par l'enregistrement des traces numériques de leur comportement, qu'ils laissent à leur insu, via leur attirail numérique ou leur avatar sur l'espace virtuel. Chaque individu écrit, sans le savoir, un journal intime éclaté, dans les registres des opérateurs, des fournisseurs d'accès à Internet, des sites web, des moteurs de recherche, que des « biographes », sortes de *big brother* ou détective masqué, risquent de reconstituer à des fins d'inquisition numérique ou de filature électronique, en dehors de toute législation.

....

(2) Corruption de TCP (Transmission Control Protocol), le protocole de transport fiable permettant à deux applications d'échanger des données, par exemple : pour éviter de « redémarrer à froid », suite à une congestion sur le réseau, rien n'empêcherait de modifier les protocoles de son ordinateur à des fins d'utilisation égoïste.

(3) La propriété numérique est complexe : dans le cas du dossier médical personnel, les données du dossier appartiennent au médecin, et non au patient qui ne peut qu'accéder à ses données de santé à caractère personnel.

La forme des attaques

Les deux chemins de la violence des attaquants

La violence numérique, prolongement naturel de la violence dans notre société, s'exprime de deux façons :

- en utilisant normalement de manière banale le support informatique afin de communiquer et d'échanger dans l'ombre (communauté de gens mafieux qui se retrouvent discrètement sur Internet, sectes qui utilisent le support informatique comme outil de propagande, de recrutement, marché noir, blanchiment d'argent sale, diffusion de fausses informations) ;
- en s'attaquant à des cibles désignées ou aveugles par l'exploitation des failles et vulnérabilités du système informatique (réseau distribué de robots logiciels furtifs offensifs, propagation de virus ou de messages intempestifs, utilisation ou création de failles informatiques pour gagner de l'argent et tromper des utilisateurs candides, blanchiment de code informatique sale via des logiciels téléchargeables, craquage de comptes informatiques de systèmes d'information peu protégés pour communiquer sournoisement sous une identité usurpée).

Les trois dimensions des cyberattaques

Les menaces informatiques s'inscrivent dans les trois dimensions, réelle, symbolique et imaginaire :

- L'attaque réelle, la délinquance informatique : on agresse, de manière aveugle ou ciblée, pour obtenir un gain réel de manière frauduleuse, récupérer ou falsifier une information dans un but criminel (fraude sur les cartes bancaires, les cartes SIM de téléphone ou les cartes de boîtiers de TNT, vol de mot de passe pour extorquer de l'argent, déverrouillage de consoles vidéos, usurpation d'identité, saisie ou falsification d'information pour de l'espionnage industriel).

L'attaque symbolique, médiatique : on attaque l'image de la cible par la médiatisation même de l'agression et

par ses répercussions sur l'opinion publique (défiguration de site web, pénétration dans un serveur informatique, guerre informatique). La publicité autour de ces attaques fait naître le doute et perdre confiance.

- L'attaque imaginaire, fictive ou simulée : on frappe l'imagination des utilisateurs à travers leur méconnaissance des systèmes. On intimide par des révélations, on gèle le comportement, on déstabilise. L'agresseur crée une peur irraisonnée ou fait semblant d'attaquer, la menace étant pire que l'exécution. On néglige trop souvent l'influence de ces attaques imaginaires. Les attaques dévoilées à grand renfort de tapage médiatique proviennent parfois des acteurs économiques, comme la supercherie du bug de l'an 2000, dans les années 1997 à 1999, contribuant à doper le marché, premier effet d'emballement avant la bulle Internet ⁴.

Un mélange des genres ou une combinaison de ces attaques est évidemment possible : leurre ou site attrape-nigaud, désinformation, déguisement de site web sous forme de cause noble pour récolter des fonds, saturation du trafic réseau pour empêcher une utilisation réelle d'un serveur (saturation des serveurs gouvernementaux d'Estonie en mai 2007, de Géorgie au début août 2008). L'attaque en déni de service pendant quelques heures des serveurs *Yahoo* et *Amazon* en février 2000, événement parfaitement anodin, fut le signal de l'éclatement de la bulle Internet en mars 2000. Ce sont aussi les inventions ou les alarmes d'informaticiens qui exposent des attaques hypothétiques, comme la faille dans les annuaires, début juillet 2008, du DNS (*Domain Name System*) par l'expert Dan Kaminsky [www.doxpara.com], qui a fait exagérément la une de journaux français.

Les nouvelles menaces, les nouvelles vulnérabilités

Les menaces et vulnérabilités actuelles

Depuis quinze ans, les grandes pannes informatiques d'infrastructures sont toujours dues, à l'origine, à des fautes de procédure dans des mises à jour irréversibles de logiciels : réparation à la hâte sans possibilité de revenir à l'état initial, déploiement d'un nouveau service réalisé sans mesurer les conséquences sur le reste des applications.

⁴ La mystification du bug de l'an 2000, avec un battage médiatique incitant à remplacer les ordinateurs et un marketing orchestré par les éditeurs de logiciel, fut relayée par les pouvoirs publics.

La faille principale de l'Internet provient de l'usurpation d'identité. On se cache le visage avec un masque dans le dessein d'être anonyme ou de prendre la silhouette d'un autre. Les agressions de ce genre ont de multiples variations : usurpation d'adresse d'ordinateur (« spoofing »), de site web (« phishing », « pharming »), invasion par déni de service (à partir d'un « botnet »), effraction de l'annuaire DNS. Par ailleurs, il ne faut pas négliger la commercialisation des attaques avec l'émergence d'une économie parallèle des producteurs-distributeurs-consommateurs organisés, avec de véritables contrats d'utilisation de botnets.

Pourtant, les vulnérabilités et les attaques informatiques ont finalement un impact assez faible. Peu de pannes gigantesques affectent la réalité. Un virus informatique n'a jamais tué personne. Le coût des dommages créés par un bug ou un virus est souvent surestimé. Les chiffres de perte des entreprises, qui figurent sous les dommages, mélangent tout : trop d'argent est dépensé par manque de compétence informatique et méconnaissance des logiciels utilisés. Il n'existe d'ailleurs pas d'assurance tout risque en dommages de système d'information, pour la composante intangible, logiciels et données.

L'image des vulnérabilités actuelles, données par certains experts ou la presse, est différente. On parle de cybercriminalité, de cyberterrorisme, de grands périls, sans jauger avec exactitude la réalité des faits. Les éditeurs de logiciel accentuent cet effet : le marché de l'antivirus en France est florissant. L'épouvantail⁵ des virus fut un message bien compris par ces éditeurs dont le mécanisme vampirise les processeurs, alors que l'intelligence des algorithmes antivirus est bien minime [Filiol, 2007].

Les menaces et vulnérabilités à venir

Les contenus illicites (pédophilie, racisme) du Web risquent d'être bientôt détrônés par des calculs illicites sur le réseau, plus dangereux encore pour le respect des individus (moteur de recherche pour fureter la sphère privée et répertoire des internautes) et la paix dans notre société (déni de service régionalisé). Des applications tentaculaires emprunteront bientôt pendant quelques minutes la puissance de votre ordinateur, tourneront à saute-mouton, sur des millions d'ordinateurs différents, pendant des années, sans que les réels propriétaires de ces ordinateurs soient informés. Les responsables de ces

applications pourront lancer des applications bienveillantes (des calculs astronomiques sur la galaxie, des applications de surveillance de tsunamis) ou des applications de cryptanalyse pour casser des codes. Ces calculs pourront être plus malsains, cruels ou destructeurs : calculs d'une bombe A pour une organisation terroriste, calculs et dissémination de milliards de virus informatiques tous distincts que les logiciels traditionnels d'antivirus ne pourront contrecarrer.

Les attaques se renouvellent ou se métamorphosent en général tous les trois ans. Tour à tour, les générations d'attaques par virus sur support physique, par virus sur fichiers attachés dans des messages, ont quitté le palmarès et laissé place à une génération de virus plus intrusive en 2003. Cette génération correspond à l'arrivée de l'ADSL en France, génération qui s'est convertie vers 2006 en des assauts de messages de désinformation et des dénis de service distribués, favorisés par l'émergence de nouveaux pays d'internautes et une nouvelle vague d'internautes néophytes, chez nous. Ces menaces se transformeront en 2009 en d'autres actes malveillants incités par les attaques des applications en pair à pair, les applications géographiques (en utilisant des applications du type *GoogleEarth* et le géoréférencement), les téléphones plus ouverts aux applications distribuées, l'interconnexion plus forte du téléphone et de l'Internet, la télévision mobile personnelle. Nul ne peut deviner quel angle d'attaque sera popularisé parmi les communautés actives des pirates.

La cybercriminalité et le cyberterrorisme

Alors que l'on discrimine bien délinquance, criminalité et terrorisme, il existe un certain flou dans l'utilisation du vocabulaire qui fait que l'on mêle dans la presse à sensation délinquance informatique ou cybercriminalité avec cyberterrorisme. Il faut faire la part des choses, l'informatique n'est pas encore intrinsèquement un support de terreur ou une arme de destruction⁶. La cybercriminalité choque les mœurs, porte atteinte à la tranquillité et à la sûreté des citoyens tandis que le cyberterrorisme fait trembler la société.

La cybercriminalité est apparue très tôt, dès que l'utilisation informatique s'est répandue auprès d'un large public dans les années 1960. Elle n'a cessé de croître.

(5) Installer une défense avec pare-feu, antivirus dans chaque ordinateur est une stratégie équivalente à dissoudre notre armée et notre police, en disant à chaque Français : « Armez-vous, payez-vous une milice personnelle ou payez des mercenaires qui agiront sans garantie de l'étranger ».

(6) On a déjà tué de manière ciblée, grâce à la géolocalisation : personnes cibles utilisant des téléphones par satellite, repérage de terroristes dans la jungle et frappe chirurgicale de ces objectifs.

Le cyberterrorisme n'existe pas encore véritablement en 2008, mais il deviendra une arme nouvelle contre nos sociétés le moment venu, si on n'y prend garde : des nuages de programmes et de données s'engouffreront alors dans une spirale violente pour tuer, ignorant les frontières des ordinateurs et des réseaux car ils atteindront fatalement les infrastructures physiques et les activités humaines.

Les conditions techniques du cyberterrorisme

Pour qu'une organisation terroriste puisse préparer de tels attentats et faire surgir ces événements sinistres, il faudrait réunir deux conditions⁷ qui conjugueraient leurs puissances néfastes :

- Il faudrait, d'une part, être capable de déployer, sur la friche informatique du réseau mondial, une infrastructure virtuelle, spontanée, transcontinentale, furtive et cohérente, c'est-à-dire mettre en mouvement des applications malveillantes anonymes sur des millions d'ordinateurs en réseau, subrepticement, de manière dynamique et continue, pendant une durée de l'ordre d'une semaine au moins, avec une puissance informatique de quelques « pétaflops⁸ ». Les grilles informatiques actuelles ne sont pas encore capables de mettre en œuvre ces propriétés de puissance, de continuité et de furtivité. Pour anonymiser leurs assauts, les attaquants mettent une capote sur les protocoles ; pour surprendre l'adversaire, les attaques informatiques se propagent à la vitesse de la lumière sur les réseaux en fibre optique, pour compliquer les enquêtes et les poursuites, les scénarios d'attaques sont internationaux, les interconnexions des réseaux transgressent les frontières, la discrétion dans les attaques devenant une propriété plus fréquente depuis que la surveillance du réseau s'organise. Mais l'intelligence des attaques artificielles est faible : ce sont des dénis de services, bruts avec une frappe massive, sans apprentissage ou adaptabilité, incapables de modifier leur comportement *in vivo*.
- Il faudrait, d'autre part, que les flux des ordinateurs interagissent directement avec la réalité physique et l'activité humaine. Ce n'est pas encore le cas en 2008. Les humains sont toujours détachés de leurs ordinateurs : entre la réalité physique et les ordinateurs, il existe encore

un maillon humain qui permet de court-circuiter la relation directe, suite à un dysfonctionnement ou une anomalie. Ce verrou risque de sauter bientôt suite à l'immersion de l'informatique dans le monde vivant, aux personnes cyberdépendantes du réseau (stimulateur de malade cardiaque, connecté à Internet), et à l'irrigation toujours plus grande de l'informatique dans l'activité quotidienne : flotte de véhicules télécommandée via le réseau⁹, téléassistance de personne fragile, surveillance des personnes géolocalisées par bracelet électronique, applications industrielles de surveillance composées de réseaux autonomes de capteurs et d'actuateurs, dispersés dans la nature.

La mise en place de caméras dissuasives de surveillance dans les lieux publics risque de chasser de la rue les terroristes qui finiront par se réfugier dans leur domicile. On risque de voir éclore dans le secret de caches privées, une communauté de cyberterroristes qui pilotera en réseau, à partir de leurs ordinateurs, une immense toile anonyme de nœuds virtuels et piégés. Les actuels botnets ne sont qu'une amorce de ce genre d'arme.

Le règne numérique chaotique

Le métasystème numérique, dans son exploitation quotidienne et dans son évolution à long terme, échappe aux technologues et aux industriels du laisser-faire, apprentis sorciers d'un nouveau *Far West*. Le profil des attaquants est souvent l'objet de fantasmes, nourris par l'appréciation ambiante, si bien que l'on a tendance à restreindre le catalogue des menaces et des scénarios d'attaques. Mafia russe pour la délinquance informatique ou « hacker » islamiste pour le cyberterrorisme sont des exemples de schématisation.

La violence légale, économique et scientifique

À côté de la violence illégale et féroce, il existe aussi un affrontement légal, la compétition brutale entre les entreprises toujours plus internationales (intelligence économique). Il ne faut pas non plus ignorer la rivalité scientifique entre les centres de recherche, la concurrence entre les pays (gestion de l'opinion publique), voire la

(7) Le but de cet article est de prévenir objectivement, de solliciter des initiatives de recherche ; il n'est pas de susciter un vent de panique ou de mettre de l'huile sur le feu.

(8) Un Pétaflops : un million de milliards d'opérations par seconde : le flops (*F*loating *P*oint *O*perations *P*er *S*econd) est la mesure de la puissance de calcul des ordinateurs.

(9) On sait déjà intercepter une voiture volée, lorsqu'elle est équipée d'un antivol à télécommande.

guerre de l'information via des services divers d'institutions légales ou des associations « sans frontières ».

Le marché de l'informatique, première industrie au monde (2 500 milliards d'euros), suscite des batailles à l'échelle des continents. Les chercheurs sous-estiment souvent cette influence majeure sur le destin des infrastructures numériques : tassement de la recherche scientifique à cause de mauvaises orientations, ralentissement des innovations dans les architectures de base à cause de l'immobilisme du marché, frein dans certains secteurs de l'informatique à cause d'une industrie dominante qui tient à conserver sa primatie et asphyxie les succès prometteurs de petites entreprises, assèchement des financements de recherche dans des secteurs innovants pour protéger des produits informatiques déjà en place.

Bien sûr, il ne faut pas confondre la violence illicite des cybercriminels avec la compétition normale des entreprises ; néanmoins si l'éthique des uns et des autres diverge, les méthodes employées se ressemblent souvent. Si les procédés sont analogues et si les pratiques ne le sont pas, les unes étant criminelles et illégales et les autres normales et admises, comment distinguer une entreprise qui affronte une autre entreprise d'un pirate qui agresse une personne privée et comment surveiller et contrôler cette surveillance ? C'est tout le problème de la politique et de l'éthique de la police du réseau.

La perte du contrôle de l'espace numérique

Tout le monde a perdu le contrôle de l'informatique, en général. Ce n'est pas le cas des industries sensibles (nucléaire, énergie, transport, agriculture, santé) qui fonctionnent avec l'informatique, car ces systèmes numériques sont très fermés aux communications extérieures et sérieusement contrôlés par des procédures rigoureuses à l'intérieur. La maîtrise de l'informatique, science de l'organisation des symboles, fait partie des grands défis de ce siècle, au même rang que l'écologie avec la maîtrise de l'énergie, la démographie et la lutte contre la misère.

Le règne numérique n'est plus contrôlé, foncièrement à cause des bugs inhérents à l'informatique actuelle, et subsidiairement à cause de l'opacité des services. D'abord, les erreurs dans les logiciels sont dues à la pauvreté de la sémantique des langages informatiques et à la faiblesse des environnements de fabrication et de validation des logiciels. Ensuite, les éditeurs de logiciels pratiquent la

non-transparence au motif de garder les secrets de fabrication. Les codes-sources des logiciels hégémoniques sont habituellement confidentiels : système d'exploitation, moteur de recherche, téléphonie sur Internet, logiciels de sécurité. La technologie informatique, bâtie sur des limons récents, est déstabilisée en permanence, par un modèle économique de l'informatique qui favorise l'innovation des services, voire la fuite en avant, plutôt que la sécurité et la sûreté de fonctionnement.

Si on sait à peine réaliser des logiciels conformes et corrects avec les langages informatiques actuels, on sait encore moins construire et faire utiliser des logiciels inoffensifs¹⁰. Un logiciel peut être parfaitement correct, conforme à sa spécification et à sa documentation, et se révéler dangereux (c'est justement le cas des vers informatiques). Un logiciel peut être incorrect et demeurer inoffensif. Il ne faut pas confondre la sécurité ou la sûreté avec les exigences de correction, de validation et de vérification, les objectifs de ces disciplines sont distincts. En sécurité, il est vain de comprendre toutes les subtilités et les effets de bord de l'horlogerie inextricable des systèmes numériques, il suffit de contrecarrer leurs actions périlleuses et les pannes par des boucliers robustes, avec des mécanismes résistants, conformes à une politique de sécurité, mais de complexité nettement plus réduite que celle du système. Enfin, les modèles de sécurité de type « bac à sable » sont insuffisamment exploités. On pourrait imaginer la mise en place de ces filets de sécurité profilés pour les utilisateurs novices, ce qui les immuniserait contre des fautes occasionnelles.

Une exploitation étendue des vulnérabilités

Les menaces résultent de tous les acteurs qui interviennent dans les édifices numériques. Ce sont des attaques intentionnelles ou simplement des erreurs, dans les deux phases distinctes de conception ou d'exploitation des systèmes. Les attaques intentionnelles proviennent statistiquement des utilisateurs du Web, mais on aurait tort de se borner à ces assaillants. Les infractions et les erreurs humaines, à l'intérieur des entreprises par du personnel autorisé, sont plus importantes que les attaques anonymes issues de l'extérieur. La panoplie des acteurs susceptibles d'engendrer ces menaces est large :

- ce sont des concepteurs de système, qui engendrent des fautes de conception par inadvertance, ou qui laissent des faiblesses après une évolution des usages ;

....
(10) Y remédier devrait être une priorité, mais la recherche en sécurité est paupérisée : on masque l'indigence de ses budgets propres, en y rattachant les budgets de la recherche en conformité du génie logiciel.

ce sont des pupitrés qui engendrent des fautes d'exploitation, suite à des défauts de procédure, par manque de formation suffisante ;

ce sont des développeurs informatiques de logiciel libre ou propriétaire, qui incrustent des bombes logicielles ou laissent des portes dérobées dans un programme informatique dans la prévision d'un déclenchement ultérieur ;

ce sont des acteurs voyous : opérateur de télécoms résolu à déstabiliser la chaîne de confiance des opérateurs de téléphone mobile ¹¹ ; fournisseur d'accès borderline décidé à attirer les clients en leur offrant des services douteux ; fournisseur de services qui héberge des contenus illicites ou qui examine le contenu de leurs clients avec l'intention de leur offrir des publicités profilées ; éditeurs de logiciels qui profitent de l'opacité de leurs logiciels pour épier le comportement des utilisateurs ; ou simplement des utilisateurs malveillants ou inconscients réalisant des téléchargements illicites ;

c'est une obscurité dans la gestion et la gouvernance des systèmes. La répartition inéquitable et la disette des adresses de l'Internet sont entretenues pour gêner l'Asie. La gouvernance hégémonique de l'Internet avec la mainmise transatlantique est une question ouverte qui risque de faire basculer tôt ou tard le réseau mondial vers une balkanisation de l'Internet. « L'harmonie » actuelle du Village global risque de se dissoudre dans une confrontation plus brutale, au profit d'un paysage moyenâgeux où l'on verra se dresser de nouvelles murailles protectionnistes.

L'abandon de la souveraineté

Les États ont perdu leur souveraineté numérique. Les éditeurs de logiciel qui vendent un système d'exploitation, le logiciel d'antivirus, les fournisseurs qui proposent gratuitement un moteur de recherche, interviennent dans le patrimoine numérique des utilisateurs. Ils ont pris en charge les utilisateurs, leur comportement (traces numériques géolocalisées par un éditeur), voire leur intimité (mots clés volés sur les moteurs de recherche). Alors que la finalité première est d'offrir un service direct (comme vendre un système d'exploitation, un logiciel pour télécharger sur Internet, une protection antivirus) à l'utilisateur final selon une spécification précise, l'éditeur du logiciel divulgue une information collatérale qui n'est pas inscrite

dans la finalité première du logiciel. Avec l'étendue massive du marché informatique auprès des citoyens, l'éditeur de logiciel, leader dans son domaine, s'octroie, statistiquement à l'échelle d'un pays, une information indirecte qui n'était pas acquise au départ. Ce point de vue à deux niveaux transforme, secondairement mais stratégiquement, cet éditeur en un acteur de métrologie informatique : statistique de l'activité digitale des utilisateurs dans une région, météo des virus ou spams du Web en France, trafic sur Internet à l'échelle d'un pays. La surveillance du monde numérique, d'ordre régalien, est maintenant sournoisement concurrencée, exploitée et accompagnée par des éditeurs privés, souvent étrangers. Une inquisition numérique sur les autoroutes de l'information occupe une place privilégiée à côté des autorités compétentes, dans tous les pays. La loi Informatique et Liberté de 1978 aurait besoin d'une sérieuse révision afin de s'adapter aux pratiques actuelles de finalité et de proportionnalité. Enfin, on devrait prohiber l'insolence des contrats inintelligibles de licence d'utilisation qui apparaissent dans les minuscules fenêtres avant une installation logicielle, que l'on doit accepter sans conditions face à des éditeurs logiciels qui ne s'engagent à rien quand on achète leur licence.

Le déficit de sensibilisation des usagers

Le marché de la sécurité informatique est difficile. Les utilisateurs, et même les entreprises, négligent ou bien ignorent les dangers potentiels. Les utilisateurs ne veulent pas s'embarrasser d'outils de sécurité trop lourds, ils dédaignent les avertissements tant qu'ils n'ont pas été confrontés à la réalité d'un dommage. Le risque d'un préjudice est jugé faible devant les opportunités si intéressantes du réseau. La législation rend en général responsable et coupable l'utilisateur final si bien que les éditeurs de logiciels sont peu enclins à améliorer la sécurité de leur produit. Dans la chaîne de confiance, la loi devrait responsabiliser davantage de manière proportionnée tous les acteurs qui contribuent à la chaîne de communication : le fournisseur d'accès, l'éditeur de logiciel qui a vendu sa licence d'utilisation. Il existe une non-responsabilité, une impunité généralisée dans le monde numérique, qui remonte à l'introduction du *copyright* en informatique. La loi qui fait porter le fardeau sur le seul utilisateur final, implique que personne ne se sent responsable de cette déficience. Cependant, il n'existe pas d'opposition entre l'économie et l'écologie numérique, entre une informatique qui serait performante et innovante et une informatique qui

¹¹ Tous les opérateurs GSM du monde sont interconnectés et inter-opèrent pour qu'un abonné connu d'un seul opérateur de télécoms puisse téléphoner de n'importe quel point de la planète.

respecterait les utilisateurs dans leur souveraineté et leur dignité.

Le déplacement de la prépondérance cryptographique

L'outil fondamental de la sécurité est la cryptographie. Ce pilier sur lequel repose toute la sécurité se fissure à cause des interconnexions robustes et massives de l'informatique ubiquitaire. En outre, sur un plan géostratégique, la suprématie scientifique occidentale dans cette discipline est en train de se déplacer vers l'Asie. La science cryptographique vacille, attaquée sur plusieurs fronts. Les fondements de la discipline sont basés sur la notion de secret et sur la mesure quantitative de la résistance d'un algorithme.

Sur le front de la connaissance, la cryptographie a été longtemps une science fermée, calfeutrée chez les militaires. Elle était, sur le plan technologique, essentiellement américaine grâce à la suprématie des algorithmes du RSA, du DES. Elle s'est ensuite disséminée dans le monde civil, à tel point que la cryptographie s'est déplacée sur l'échiquier politique. L'AES, le dernier algorithme de chiffrement par blocs est belge (université de Louvain). Le dernier théorème sur les nombres premiers a été démontré en Inde, à Kanpur, en août 2002, (sur le caractère polynomial du calcul pour déterminer la primalité d'un nombre entier) [Agrawal, 2004, p. 781], et Xiaoyun Wang de l'université de Shandong en Chine a montré des attaques par collision des fonctions de hachage MD5 et SHA-0 à la conférence CRYPTO'04, et cassé, en février 2005, les algorithmes de hachage qui sécurisent l'Internet actuel.

Sur le front des moyens informatiques, il faut posséder, pour casser un code secret, une puissance informatique extraordinaire, démesurée vis-à-vis des adversaires. Cette puissance était l'apanage des gouvernements ; ils pouvaient mesurer leur force à l'aune de la puissance informatique, cette force brute qui permet de percer un secret, en y mettant les moyens. Ce temps sera bientôt révolu pour deux raisons essentielles.

D'une part, certaines applications civiles, comme les moteurs de recherche pour l'indexation des mots, requièrent une concentration exceptionnelle de serveurs informatiques, à tel point que des fermes d'ordinateurs pullulent sous des hangars, expansion visible sur l'évolution temporelle des images de *Google Earth*. Deux ou trois entreprises informatiques monopolisent à elles seules

plus du tiers de la puissance de calcul et de stockage des serveurs de la planète. Cette puissance concentrée pourrait être détournée le moment venu. D'autre part, un individu quelconque pourra bientôt, à partir de sa chambre, se connecter et fabriquer un tissu d'arlequin de serveurs connectés pour calculer ses propres applications.

La cryptographie risque de n'engendrer bientôt que des secrets de Polichinelle. Il est temps que la science cryptographique se renouvelle, arrête de n'utiliser que la force brute des ordinateurs, et s'ancre aussi sur la réalité : l'histoire, le passé ou l'évolution dans le temps des secrets, la géographie ou la place des réseaux, la configuration des ordinateurs, bref des secrets réels laissés çà et là sur la lande informatique. La cryptographie quantique paraît être aussi une promesse intéressante pour distribuer ces secrets.

Le chantier d'une nouvelle urbanisation numérique

L'Internet s'est brisé

Ce que les spécialistes savaient déjà depuis longtemps, David Clark l'a révélé en décembre 2005 au grand public : « *Internet is broken* » [2005]. L'Internet s'est fracassé à cause de son architecture trop ancienne et son gigantisme ; il ne s'est adapté ni à la mobilité, ni à une sécurité moderne. Les outils de protection existent, mais ils ne sont pas ou peu utilisés, n'ont pas le succès escompté ou bien coûtent trop chers. Les infrastructures de gestion de clés publiques sont peu déployées puisque le marché de l'administration des certificats est faible, la signature électronique n'est quasiment jamais utilisée malgré les directives européennes, le déploiement de la biométrie nécessite un énorme investissement de départ d'enregistrement canonique de confiance. Seuls les antivirus ont du succès, trop sans doute. La cryptographie est peu utilisée pour le chiffrement de données, dans les applications normales. Les échanges téléphoniques sont en clair, le GSM chiffre, seulement dans certains pays, le segment des communications dans l'air. Les échanges par messagerie électronique sont en clair, si bien que des communications chiffrées deviennent suspectes. Cependant, il ne faudrait pas grand-chose pour que tout bascule. La téléphonie sur Internet via *Skype* est chiffrée. Les applications P2P pourraient bientôt être chiffrées. Mais ces chiffrements de données, s'ils protègent la transmission, ne vont pas forcément rassurer les interlocuteurs des échanges, qui ne partagent pas les secrets de ce codage. C'est évidemment celui qui exploite le service qui maîtrise tout.

Un Internet polymorphe et multipolaire

Dans le futur, on va assister à une informatique de plus en plus abstraite. On ne pourra plus raisonner en termes de monotéchnologies. L'Internet du futur sera polymorphe, créé à partir de plusieurs infrastructures différentes, fragmenté géographiquement selon une gouvernance multipolaire. On sera probablement dans un schéma de recouvrement de l'ubiquité de l'espace informatique, un peu comme des tapis successifs de feuilles d'automne qui recouvrent le sol de la forêt. Il existera un premier socle de transmission avec la fibre optique et la radio. Il existera une deuxième couche de communication, avec non pas des routeurs ou des commutateurs, mais de véritables ordinateurs différents, spécialisés, selon leur emplacement dans le réseau. Il existera enfin un troisième socle, celui des applications et des services, avec les données.

L'enjeu principal de l'Internet du futur est donc de maîtriser ces infrastructures de communication : gouvernance de l'Internet, maîtrise des opérateurs de télécoms, de télévision, souveraineté sur les infrastructures de géolocalisation, contrôle de l'Internet des Choses.

Un nouvel horizon pour des paradigmes modernes

L'actuelle vision des chercheurs américains GENI [www.geni.net] ou européens FIRE [cordis.europa.eu/fp7/ict/fire/] tient dans l'idée établie qu'il faut construire des systèmes toujours plus complexes, plus interconnectés, entrelacés mais sans couture, supportant sans difficulté une forte hétérogénéité, presque auto-administrables, baignant dans une ambiance mobile, intelligente, peuplée de logiciels ubiquistes, saturés d'informations omniprésentes, avec des utilisateurs capables de se connecter presque partout et en permanence, nomades, sans contrainte de sédentarité, actualisant leurs programmes informatiques en ligne, téléchargeant les mises à jour de sécurité.

Il faut d'abord dépasser la démarche de l'informatique, une conception incrémentale des réseaux du futur, et notamment de l'Internet, empreinte d'optimisme comme une méthode Coué et d'une orthodoxie conservatrice. Un bouleversement éventuel (en termes géostratégiques, économique, technologique) est une variable à intégrer, car une rupture historique, concevable dans les deux décennies à venir, pourrait conduire jusqu'à un désordre international majeur.

Il faut enfin incorporer la rupture, la nature dynamique et évolutive des systèmes numériques. Nos repères informatiques actuels sont en train de se dissoudre. Les dichotomies entre l'ordinateur et le réseau, le matériel et le logiciel, les applications et les services, le plan logique et le plan virtuel, les logiciels et l'information, sont en train de s'estomper, ou, plus exactement, les termes de la césure changent radicalement de signification. La feuille de route de l'architecture des réseaux suit le même itinéraire que l'histoire des langages informatiques, avec une complexification du typage des abstractions.

Modèle, contre-modèle, alter-modèle

Dans la recherche informatique internationale [www.inco-trust.eu], il faut susciter une pensée intercontinentale. Les pensées du monde sont sans doute localisées : il faut donc penser la différence, les modèles de l'altérité. Avec la mondialisation, il faudra accepter les innovations mais aussi les détournements et les reprises d'inventions. Il faudra alors concevoir d'autres références avec des modèles, des contre-modèles et des alter-modèles et inventer des passerelles entre ces modèles, suite à l'arrivée sur la scène informatique de la Chine et de l'Inde. On dit parfois que le XIX^e siècle fut européen, le XX^e fut américain, le XXI^e sera asiatique. Il se produit indubitablement une mutation des préoccupations, à la fois démographiques et de développement, un déplacement de pouvoirs dont il faudra tenir compte, y compris dans la science et la technologie. Il faudra aussi intégrer les mouvements de contestation, à la fois des mouvements pseudo-libertaires (les « naïfs de l'Internet ») et des purs et durs de la répression (les gouvernements autoritaires). On verra se greffer sur le réseau physique mondial, universel, sans frontières, une multitude de services, à l'intérieur de murs virtuels, avec des propriétés à la carte : infrastructure de confiance laxiste, réseau marchand, réseau sécuritaire. Tout ne sera pas résolu avec cette fragmentation du filet de l'interconnexion, loin s'en faut.

Dans une perspective de laisser-faire la technologie, on risque de rester descriptif de l'ordre : on ne maîtrise pas l'évolution, la régulation est autoréflexive, on évite ainsi de passer au normatif. Gouverner, c'est définir un ordre. En matière de technologies, on décrit trop souvent ce qui est, et pas assez ce qui devrait être ou ce qui pourrait être, sans même s'ouvrir à des démarches qui acceptent l'utopie : un « ONU numérique » rentrerait dans le champ de cette utopie.

La balkanisation du Village

Avant la convergence, les infrastructures de communication étaient séparées. Les cloisons étanches entre l'Internet, le téléphone et le téléviseur diminuaient la probabilité de panne en cascade des trois systèmes.

De nouvelles infrastructures vont naître. Les infrastructures de géolocalisation (Galileo en Europe, GPS aux États-Unis, Glonass en Russie, Beidou-2 en Chine, IRNSS en Inde) se mettent en place, et esquissent le nouveau Yalta numérique du XXI^e siècle : Amérique du nord, Europe, Russie, Chine, Inde, Brésil. Dans l'avenir, l'heure et la position de confiance vont fortement structurer l'informatique et leurs services avec des services géolocalisés. Les infrastructures de géolocalisation sont un atout supplémentaire de la sécurité : on remet les pendules à l'heure et l'on pointe les boussoles au même nord. Les millions d'ordinateurs qui avaient des horloges différentes et peu fiables vont désormais utiliser la même heure. On va pouvoir acheminer des paquets d'informations selon la latitude et la longitude, on va pouvoir déployer des protocoles cryptographiques et authentifier un sujet, un objet en fonction de son identité, mais aussi de sa position à l'heure dite : cet attribut va permettre de crédibiliser un échange commercial, authentifier une personne qui veut se connecter à l'ordinateur de son entreprise à partir de son domicile. Cette fonction inédite va créer des alibis par l'enregistrement du trajet. L'informatique va réinvestir le monde réel.

La pollinisation des services

Les services aujourd'hui sont attachés et verrouillés à leur infrastructure. On va assister à un déverrouillage des services et des applications qui vont se libérer de leur infrastructure originelle. Telle application qui se déployait jadis sur la télévision va se déployer sur l'Internet ou le téléphone. Mais plus encore, on va assister à la création de nouveaux services qui seront à califourchon sur plusieurs infrastructures : des services virtuels spontanés vont se créer en prenant l'heure et la position sur Galileo, des tags de l'espace environnant sur l'Internet des Choses, une application par un programme Java sur un site Web2 de l'Internet courant, des données personnelles sur la carte SIM du téléphone portable, et utiliseront des éléments d'une émission de télévision interactive. Les nouveaux services informatiques seront des bulles intangibles qui surnageront sur le maquis des infrastructures de communication. On va assister à une pollinisation des services qui vont opérer une fertilisation croisée : la difficulté sera de maîtriser ces boutures informatiques. La sécurité et la

sûreté du système devront reposer sur une approche holistique, pour empêcher des effets dominos [Riguidel, 2003].

Par-delà l'inéluctable

L'interdépendance de la vie quotidienne envers les infrastructures vitales est préoccupante. Le cyberspace, assemblage délicat et dynamique de deux ensembles dispersés de logiciels et d'informations, constitue une vulnérabilité majeure dans nos sociétés. Les attaques et les pannes dans ce règne numérique découlent de l'architecture en pièces rapportées, des logiciels opaques et fragiles, et des données en expansion continue. Ces faiblesses sont exploitées par la violence des délinquants, des criminels ou des terroristes. Elles sont favorisées par le manque de sensibilisation des utilisateurs, et accentuées par une gouvernance déficiente, une jurisprudence absente. Comme les technologies deviennent globales, les menaces se mondialisent, elles aussi. Sans décellement précoce, une attaque distribuée, peu dangereuse au premier abord, mais prenant de l'ampleur avec son évolution, comme une vague qui déferle lentement, pourra se révéler désastreuse. L'identification *in vivo* de l'attaque sera impossible. Il faut donc inventer dès maintenant, des instruments de sécurité, opérés par des instances légales comme un dispositif réticulaire robuste qui s'autocritrise en rétrécissant ses tuyaux automatiquement afin de ne véhiculer que les messages urgents, et qui se protège en ripostant de manière graduée par des contre-attaques. Comme pour toute prévention, il faut renforcer le renseignement informatique légal (infiltration, écoute), contrôlé démocratiquement, couplé avec le travail classique sur le terrain. Le travail sur ces menaces futures ne doit pas affaiblir les luttes plus concrètes sur les fléaux actuels : marché de la drogue, prostitution, sectes en tout genre attirées par l'argent facile, organisations criminelles camouflées sous des allégations politiques, gerbe de mondes parallèles qui se recourent tout près de nous, dans l'ombre. La confrontation à la barbarie numérique à venir ne pourra être séparée de la lutte acharnée contre le terrorisme et le rude combat contre la criminalité. Dans un monde violent et globalisé, le repère de nos valeurs, la défense de nos principes et de notre modèle devront guider notre action afin d'organiser sainement le renseignement numérique et protéger l'indépendance, la souveraineté et l'intégrité du patrimoine numérique des citoyens, des entreprises et de notre pays, en parallèle avec la lutte offensive contre la criminalité, le trafic de drogue et la corruption.

Michel RIGUIDEL

DOCUMENT N°3

Cybercriminalité

Le terme « cybercriminalité » a été inventé à la fin des années quatre-vingt-dix, alors qu'Internet se répandait en Amérique du Nord. Un sous-groupe des pays du G8 fut formé suite à une réunion à Lyon, en France, afin d'étudier les nouveaux types de criminalité encouragés par, ou migrant vers, internet. Ce « groupe de Lyon » employait alors « cybercriminalité » pour décrire, de manière relativement vague, tous les types de délits perpétrés sur internet ou les nouveaux réseaux de télécommunications dont le coût chutait rapidement.

En même temps, et à l'initiative des membres du groupe de Lyon, le Conseil de l'Europe commença à rédiger un projet de Convention sur la Cybercriminalité [1]. Cette convention, rendue publique pour la première fois en 2000, prévoyait un nouvel ensemble de techniques de surveillance que les organismes chargés de l'application de la loi estimaient nécessaires pour combattre la « cybercriminalité ». Comment la cybercriminalité était-elle définie? La version finale de cette convention, adoptée en novembre 2001 après les événements du 11 septembre, n'en proposait pas de définition. Le terme était plutôt utilisé comme une sorte de fourre-tout pour désigner les nouveaux problèmes auxquels se trouvaient confrontés la police et les agences de renseignement, et découlant des performances toujours meilleures des ordinateurs, de la baisse du coût des communications, et du phénomène Internet. La convention énumère les différentes dispositions et les domaines exigeant une nouvelle législation :

Titre 1 - Infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques.

Titre 2 - Infractions informatiques [falsification et fraude].

Titre 3 - Infractions se rapportant au contenu [pornographie].

Titre 4 - Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes.

Titre 5 - Autres formes de responsabilité et de sanctions [aide et complicité, responsabilité des personnes morales].

Cybercriminalité : la boîte de Pandore

Les dispositions relatives aux crimes sont en réalité très brèves, la majeure partie de la Convention traitant de droit procédural et de coopération internationale. Pour que les poursuites aboutissent, il fallait trouver de nouvelles techniques pour réunir des preuves, assurer leur intégrité, et les partager par delà les frontières. Les injonctions de conservation rapide de données stockées, les mandats électroniques, le recueil de données en temps réel, l'archivage des données relatives au trafic : autant de mesures qui impliquaient une intrusion dans les libertés civiles. Une dépendance croissante des traités mutuels d'assistance légale, même quand il ne s'agissait pas d'un cas de double incrimination, ouvrait une boîte de Pandore d'accusations criminelles possibles selon tous les régimes du monde. Alors que la Convention sur la Cybercriminalité énumère clairement les problèmes propres aux enquêtes criminelles au niveau mondial, elle ne propose toujours pas de solution pour protéger la vie privée et les droits humains.

À l'origine, il régnait une grande confusion. La notion de cybercriminalité était appliquée à de nouveaux types de criminalité, comme la cyberpornographie - c'est-à-dire la diffusion de photographies violant les lois de certains pays (mais pas tous) relatives à la pornographie inacceptable et l'exploitation des personnes. Comme internet ignore les frontières, il était devenu beaucoup plus facile de diffuser des contenus à l'étranger, parfois de manière complètement anonyme. Pénétrer dans les systèmes informatiques, ou les « pirater », constituait aussi un nouveau crime, alors que de nombreux pays ne le considéraient pas encore comme une infraction criminelle. La Convention sur la Cybercriminalité visait entre autres à établir et harmoniser les dispositions qui devaient être intégrées dans la législation des pays signataires, afin de lutter de manière bien coordonnée contre cette nouvelle activité criminelle. Les jeux d'argent en ligne soulevaient un autre problème : des champs de courses virtuels fleurissaient sur internet, et bien que les pays aient des approches très différentes, suffisamment de pays développés intégraient les revenus tirés des jeux d'argent dans les budgets nationaux et les économies du tourisme, de sorte que l'émergence de concurrents virtuels, opérant depuis des paradis fiscaux, suscitait une réelle inquiétude.

Archivage des données informatiques, cryptographie : deux grands problèmes de sécurité en question

Avant que la Convention sur la Cybercriminalité ne soit rendue publique, des défenseurs des libertés civiles du monde entier se battaient déjà contre différentes initiatives nationales visant à introduire l'archivage obligatoire des données informatiques, ou le stockage des données de connexion sur les télécommunications et le trafic Internet, à des fins d'enquêtes criminelles. L'archivage des données de connexion faisait partie d'un ensemble de mesures de contrôle présentées dès 1992 par le FBI comme nécessaires pour combattre le crime sur la nouvelle « autoroute de l'information » - comme on appelait alors Internet. Pendant toutes les années quatre-vingt-dix, des activistes d'internet, des experts techniques, et des entreprises privées avaient œuvré ensemble contre l'imposition de mesures de contrôle de la cryptographie, y compris des projets de dépôt des clés auprès d'un tiers de confiance, dans lesquels le gouvernement aurait détenu une copie de toutes les clés cryptographiques afin d'enquêter et de trouver plus facilement des preuves sur les activités criminelles. Le projet le plus célèbre fut le « Clipper Chip » américain, qui prévoyait non seulement que le gouvernement détienne les clés de chiffrement, mais qui proposait aussi un algorithme fermé ou propriétaire qu'aucun expert n'était autorisé à analyser ni tester. La sécurité est une course aux armements, dont les algorithmes et les mesures de surveillance nécessaires à son succès sont attaqués aussi rapidement qu'ils sont mis en place. En conséquence, les seules mesures de sécurité auxquelles les experts font

confiance sont celles qui ont été exposées aux attaques et qui ont survécu. À l'origine, la cryptographie relevait du domaine des experts de l'armée et de la sécurité nationale, mais de plus en plus les civils se sont mis à l'étudier et elle s'est répandue dans l'usage public.

En 1991, le pacifiste et expert en cryptographie Phil Zimmerman déposa sur Usenet un logiciel de cryptographie appelé Pretty Good Privacy, ou PGP, le mettant ainsi à la disposition de pays vers lesquels les États-Unis refusaient d'exporter une cryptographie forte. Le gouvernement américain demanda une enquête du Grand Jury, laquelle dura trois ans avant de se clore en janvier 1996 par un non-lieu. Phil Zimmerman devint un héros au sein de la communauté d'internet, étant donné qu'il avait aidé des dissidents politiques de pays comme la Lettonie à crypter leurs communications et passer outre la surveillance de leur gouvernement. Toutefois, pendant trois ans, il encourut une peine de prison pour avoir exporté un produit cryptographique.

Ce statu quo sur l'exportation des produits cryptographiques se prolongea plusieurs années, parce que l'on se trouvait dans une impasse classique : s'il ne faisait aucun doute qu'un individu pouvait entièrement dissimuler un crime économique à l'aide d'une cryptographie forte et inviolable, il était également vrai qu'une entreprise avait besoin de se protéger de l'espionnage industriel et des intrusions criminelles en utilisant le même type de cryptographie forte. Même Clipper chip fit long feu, et les États-Unis et les autres pays du G8 assouplirent leurs mesures de contrôle de la cryptographie, presque au moment de la naissance de la Convention sur la Cybercriminalité. Toutefois, l'ambiance entre les défenseurs d'internet et les experts s'était quelque peu teintée de méfiance, suite aux tentatives gouvernementales pour mettre fin au respect de la vie privée et au chiffrement sur Internet. Un bras de fer capital venait de s'engager, entre d'une part l'État, qui souhaitait pouvoir prendre connaissance de tout ce qui circulait sur les réseaux de télécommunications, et notamment Internet, et d'autre part l'individu (représenté par les groupes de libertés civiles), qui n'avait pas le sentiment que le gouvernement cherchait vraiment à le protéger, mais qu'il essayait plutôt d'asseoir son pouvoir au commencement de la nouvelle ère de l'information, en mettant en place des systèmes de surveillance qui allaient se multiplier et menacer nos libertés.

La cybercriminalité n'est pas virtuelle

Mais enfin, qu'est-ce que la cybercriminalité? Et tout d'abord, qu'est-ce que le cyberspace? Le terme a été inventé par l'auteur de science-fiction William Gibson en 1982, et appliqué à Internet par Howard Rheingold, de sorte qu'il a fini par désigner cette nouvelle infrastructure de communication. Toutefois, nous oublions parfois que le cyberspace n'a pas d'existence réelle. Concrètement, il existe un réseau, et de nombreux serveurs et équipements divers, mais les communications sur Internet semblent éphémères et insaisissables, et dans l'esprit du public, c'est là gestalt qui agit. Ceci s'explique peut-être par la fragilité de la relation entre l'individu moyen et son ordinateur ou son logiciel de courrier électronique. Qui n'a jamais perdu un document parce qu'il avait oublié de l'enregistrer, ou n'a jamais eu à déplorer la disparition de son agenda et de son courrier électronique? En réalité, un fin limier armé des bons outils peut retrouver et exhumer presque tout, parce que contrairement au monde analogique, le monde numérique laisse des traces pour chaque bit d'information et chaque octet envoyé. Ces outils et compétences ne sont pas à la portée de l'utilisateur de base, ce qui explique pourquoi la notion de cyberspace, une sorte d'hyperespace magique depuis lequel les informations vont et viennent, semble parfaitement convenir.

Au moment de commencer à rédiger le projet de Convention sur la Cybercriminalité, la plupart des organismes chargés de l'application de la loi accusaient aussi un certain retard technologique. Ils ignoraient comment enquêter, comment saisir des preuves sur des ordinateurs sans les contaminer, comment préserver l'intégrité des données dans le cas où leur propriétaire aurait envoyé une commande kill à distance pour les détruire, comment remonter jusqu'aux auteurs d'un message, notamment s'agissant de messages cryptés ou utilisant un anonymiseur. Il s'agit là de problèmes complexes, et le travail des organismes chargés de l'application de la loi se résumait à l'origine à tenter de ralentir la cadence et attirer l'attention sur leurs propres besoins en moyens pour s'attaquer à un nouveau problème. Comme il est souvent plus facile d'obtenir de nouveaux moyens pour combattre un nouveau problème plutôt que l'intensification d'un problème ancien, il n'est pas étonnant que de nouveaux termes aient été créés. Toutefois, on peut s'interroger sur l'utilité du terme « cybercriminalité », et il peut s'avérer trompeur. Les crimes se produisent en effet dans le monde réel, et impliquent généralement des personnes et de l'argent tout aussi réels. Il est important de se concentrer sur cet aspect du problème plutôt que sur les aspects plus éphémères comme les techniques d'envoi des communications.

La « cybercriminalité » se caractérise par trois aspects

Tout d'abord, il y a le nouveau crime consistant à pirater, s'introduire ou espionner les systèmes informatiques d'autres personnes ou organisations. Les opinions divergeaient quant à savoir si le simple fait de regarder était un crime, d'autant que les tout premiers « bidouilleurs » (hackers)[2] détectaient souvent des brèches dans la sécurité des systèmes et avaient le sentiment d'être des citoyens tout à fait respectables en les signalant. Cela n'a de tout évidence rien à voir avec le fait de pénétrer dans un système dans un but criminel.

Ensuite, il y a les cas dans lesquels le crime est ancien mais le système est nouveau, comme dans le cas des tentatives d'escroquerie par internet. Les arnaques commerciales existent depuis toujours, les arnaques

téléphoniques depuis des décennies, et nous avons aujourd'hui les arnaques par internet. Il en va de même pour la pornographie et le non-respect du copyright.

Le troisième aspect concerne l'enquête, dans laquelle l'ordinateur sert de réservoir de preuves, indispensables pour que les poursuites engagées dans le cadre de n'importe quel crime aboutissent. Ce qui autrefois était consigné sur le papier a toutes les chances d'être aujourd'hui consigné sous forme numérique, et peut être détruit ou chiffré à distance.

Le chien policier doté d'un bon flair semble habiter un univers parallèle... Il peut vivre avec nous et marcher dans la même rue que nous, mais il ressent les choses d'une manière complètement différente de celle d'un humain et vit dans un monde riche en informations de type chimique. L'homme a désormais construit un monde où les puces de silicium génèrent de nouvelles informations, les envoient autour du monde dans des flux électroniques numériques, et nous sommes incapables de les détecter sans l'aide des ordinateurs. Néanmoins, ce monde numérique parallèle existe, et les bits numériques constituent un nouveau type de preuves. Les bits numériques représentent aussi un nouveau type de danger pour l'individu, parce qu'une personne capable de manipuler les preuves numériques peut créer un nouveau personnage numérique, ou persona. Il s'agit d'un quatrième type de crime, plus subtil que les autres, et que l'on connaît mieux sous le nom d'usurpation d'identité. Si cette tendance persiste, « cybercriminalité » pourrait bien devenir un terme utile pour décrire les infractions commises contre la persona numérique.

La persona numérique

Qu'appelle-t-on « persona numérique », et s'agit-il d'un terme utile? L'expression est employée depuis au moins une dizaine d'années, pour désigner l'impression qu'une personne laisse sur Internet. Le Dr. Roger Clarke l'a très bien expliqué dans le résumé d'un article consacré à ce sujet. [3]

La persona numérique correspond au profil d'un individu établi par la collecte, le stockage et l'analyse des données informatiques lui correspondant. Il s'agit d'un concept très utile et même d'un concept nécessaire pour arriver à comprendre le comportement du nouveau monde en réseau. Cet article présente la notion, retrouve ses origines et apporte des exemples de son application. Nous pensons que cette notion permettra de comprendre, ou de mieux comprendre, de nombreux aspects du comportement du réseau.

La persona numérique est aussi un phénomène potentiellement menaçant, dégradant, voire socialement dangereux. Sa dangerosité potentielle réclame une attention particulière dans le domaine de la surveillance des données informatiques, c'est-à-dire l'observation des personnes au moyen de leurs données personnelles. La surveillance des données informatiques constitue un moyen économiquement efficace pour contrôler le comportement des individus et des sociétés. La manière dont la persona numérique participe à la compréhension de techniques particulières de « dataveillance » comme la classification et le profilage par ordinateur fait débat, et nous mettrons en évidence les risques propres à une observation des personae numériques.

Onze ans plus tard, nous avons progressé jusqu'à un point dérangeant annoncé dans l'article: Clarke identifie la persona numérique comme une construction, utile pour comprendre l'ombre que nous projetons dans le monde numérique du cyberspace, et il établit la distinction entre personae passives, actives et autonomes :

La persona numérique est un modèle de la personnalité publique d'un individu basé sur des données informatiques et entretenu par des transactions, et visant à servir de personnalité par procuration à cet individu.

Utiles pour construire l'identité des individus dans le but de s'adresser à eux (les adresses électroniques, par exemple) ou de les identifier comme personnes autorisées à réaliser certaines actions (payer des factures en ligne, préparer un voyage), les bits dessinent rapidement un ensemble d'habitudes et une personnalité aussi réelles que l'être humain qui se cache derrière. Les gouvernements et les entreprises les utilisent désormais pour « connaître leurs clients » et l'on fait quasiment plus confiance aux preuves électroniques et personae numériques qu'aux individus eux-mêmes.

Toutefois, des faiblesses dans la sécurité montrent de plus en plus que cette confiance est peut-être mal placée. Le « hameçonnage » (phishing) [4] et les attaques de pharming, ou la mystification de courrier électronique et de sites web, convainquent les personnes de donner des informations personnelles par internet, et les fraudeurs utilisent ensuite ces informations pour faire croire à un commerçant, un gouvernement, ou une banque qu'ils sont la vraie personne. Les voleurs poussent parfois plus loin la complexité du monde actuel, et il arrive qu'ils amalgament différents groupes de données informatiques pour créer des personnes fictives mais paraissant réelles.

N'importe où dans le cyberspace, un nombre incalculable de ces personnages fictifs pourrait sévir, généralement avec des intentions criminelles, mais pas toujours. Les représentants des forces de l'ordre se font passer pour des enfants dans des salons de clavardage dans le but d'arrêter les pédophiles potentiels. Des clients fantômes testent les services à la clientèle. Des adultes du monde entier se créent des personae sur les sites de rencontres par internet, pour cacher leur véritable identité jusqu'à ce qu'ils aient suffisamment confiance en les inconnus avec qui ils parlent.

Alors que nous nous acheminons vers un monde où la surveillance numérique des êtres humains se développe de manière exponentielle, il faut nous demander où nous allons. Bientôt, les puces d'identification par radio-fréquence (puces RFID) de nos vêtements et de nos cartes d'identité communiqueront avec notre environnement, et des émetteurs intégrés suivront nos moindres mouvements. Si quelqu'un réussit à imiter ces indices, un être humain réel

pourra se retrouver confronté devant les tribunaux à une persona numérique, construite avec soin à l'insu de l'individu concerné. Les tentatives pour établir le rapport entre ces indices et l'individu par la biométrie peuvent aider à résoudre le problème, ou bien l'empirer. Les spécialistes des libertés civiques s'inquiètent de l'omniprésence des lecteurs biométriques dans notre vie quotidienne, affirmant qu'ils ne sont pas fiables et produisent beaucoup trop de faux positifs et de faux négatifs. Une expérience récente consistant à relever des empreintes digitales et à les reproduire sur de faux doigts moulés à partir d'oursins en gélatine a confirmé qu'il était possible de duper les lecteurs d'empreintes digitales, mais elle n'a pas réussi à ralentir l'installation des systèmes [5].

Roger Clarke, dans son article sur la Persona Numérique, se réfère à la construction de l'être selon Jung, avec l'anima tournée vers l'intérieur face à l'inconscient, et la persona tournée face au monde. À mesure que la persona numérique acquiert une importance sociale et économique qui ne cesse de croître, elle attire l'attention des criminels. Alors que l'individu se trouve pris dans une course aux armements numériques pour le contrôle de sa propre persona, plutôt que de la laisser aux mains du marché ou des criminels, que devient l'anima? Si l'individu est obligé de se dissocier de sa persona, uniquement en réaction à la surveillance et à la menace constantes qui sont devenues notre lot quotidien, cela n'augure rien de bon pour notre santé mentale collective.

27 février 2006

Ce texte est extrait du livre *Enjeux de mots : regards multiculturels sur les sociétés de l'information*. Ce livre, coordonné par Alain Ambrosi, Valérie Peugeot et Daniel Pimienta a été publié le 5 novembre 2005 par C & F Éditions.

Le texte est sous licence Creative Commons paternité, pas d'utilisation commerciale.

Le cadre d'analyse

Un monde numérique particulièrement vulnérable à la criminalité

Solange GHERNAOUTI-HÉLIE*

« Cybercriminalité et sécurité intérieure : état des lieux et éléments de prévention », in M. Cusson, M. Dupont, F. Lemieux (dir.), *Traité de sécurité intérieure*, Montréal, © Éditions Hurtubise HMH, coll. « Cahiers du Québec : Droit et Criminologie », 2007, pp. 246-249 (extraits).

À l'aube du ^{xx}e siècle, l'information constitue le patrimoine numérique des nations et des organisations. L'information manipulée, traitée par les ordinateurs, communiquée grâce à des réseaux de télécommunication, est à considérer comme une ressource stratégique autour de laquelle se développe la société de l'information. Moteur de l'économie, l'information est un bien immatériel qui nécessite une protection à la hauteur des enjeux de sa maîtrise par les États et organisations.

La sécurité informatique touche à la souveraineté des États, à la sécurité intérieure, au patrimoine culturel des nations, à la protection des infrastructures critiques, des systèmes, des réseaux, des biens et des valeurs. Dorénavant, la sécurité des personnes relève également de la sécurité informatique dans la mesure où toute activité humaine dépend de systèmes de traitement de l'information. (...)

Tout dysfonctionnement informatique potentiel, quelle que soit son origine – accident, erreur, malveillance –, constitue un risque opérationnel dans la mesure où il en résultera un « risque de pertes dû à l'inadéquation ou à l'échec de processus internes, du personnel et de systèmes ou provenant d'événements externes », comme nous le rappellent les accords de Bâle II (1).

Les technologies Internet sont omniprésentes et deviennent des vecteurs incontournable de la réalisation de toutes sortes d'activités. Ainsi, le nouvel ordre numérique qui est en train de prendre forme s'exprime au travers du cyberspace qui modifie les traditionnelles frontières temporelles et géographiques, le mode de fonctionnement des institutions, mais aussi les modes d'expression et de réalisation de la criminalité.

La valeur réelle ou symbolique de l'information est devenue un objet de la criminalité. Les infrastructures, les réseaux, les systèmes, les

* Directrice de l'Institut d'informatique et d'organisation (INFORGE), professeur à l'école des HEC, Université de Lausanne.
1 Accord de Bâle II Banque des règlements internationaux (BRI) 15 juillet 2004.
Dispositif prudentiel destiné à mieux appréhender les risques bancaires.

services, les données informatiques constituent de nos jours le moyen de réaliser des délits (l'informatique comme instrument du crime) et également les cibles d'actions délictueuses (l'informatique comme cible du crime). Quel que soit le nom retenu pour exprimer cette criminalité : crime informatique, électronique ou cybercrime lorsque les technologies Internet sont impliquées dans sa réalisation, il s'agit de crimes complexes liés aux technologies de sauvegarde, de traitement et de communication de l'information. En 1983, l'Organisation de coopération et de développement économiques (OCDE) a défini l'infraction informatique comme étant tout comportement illégal, immoral ou non autorisé qui implique la transmission ou le traitement automatique de données.

Fragilité d'un monde numérique mis en réseau par des technologies universelles

L'uniformisation du monde de l'informatique et des télécommunications par l'adoption universelle des technologies Internet, la dépendance des organisations et des États à ces mêmes technologies, et l'interdépendance des infrastructures critiques introduisent un degré de vulnérabilité non négligeable dans le fonctionnement des institutions publiques et privées. Cela peut mettre en péril leur pérennité, mais aussi la souveraineté des États. (...)

Les infrastructures informatiques et de télécommunication sont vulnérables du fait de leurs caractéristiques, puisque la vulnérabilité fondamentale du numérique provient de la séparation de l'information et de son support physique.

La technologie permet la séparation entre le contenu d'une information (sa représentation et sa signification) et son contenant, c'est-à-dire le support physique sur lequel le contenu est temporairement transcrit (mémoire vive, disque dur, cédérom, fibre optique d'un réseau, onde hertzienne de transport, etc.). En devenant immatérielle, l'information numérique devient indépendante de son support, volatile et fragile.

Ainsi par exemple, une donnée peut être détruite, modifiée, copiée, volée indépendamment de son support, par un processus informatique, et ce, à distance. De plus, la notion de donnée d'origine n'a plus de sens, puisque les copies à l'identique et à l'infini sont possibles. (...)

La mise en réseau des ressources grâce aux technologies Internet font qu'elles deviennent des cibles faciles et attrayantes pour la réalisation de délits, ce qu'ont bien compris les adversaires des organisations et des États pour les déstabiliser ou obtenir des bénéfices économiques.

Les technologies de l'information profitent aux criminels

Outre des vulnérabilités inhérentes à tout système complexe, des outils d'attaque de systèmes sont disponibles sur le Net pour porter atteinte à l'intégrité, à la disponibilité ou à la confidentialité des ressources.

Des outils d'exploitation des vulnérabilités des systèmes et de logiciels capitalisant le savoir-faire criminel dans un programme (logiciels automatisés de piratage) donnent à l'internaute la capacité potentielle de devenir, selon sa motivation et les cibles attaquées, cybercriminel ou cyberterroriste.

Par ailleurs, le fait de pouvoir localiser des serveurs dans des États faibles, qui constituent des refuges pour des opérations transnationales, ainsi que le manque de régulation internationale et de contrôle du réseau Internet permettent aux criminels une prise de risques minimale. Ainsi, le criminel tire parti de l'aterritorialité du réseau Internet, de l'inexistence dans certains États de lois réprimant le crime informatique et des juridictions multiples dont relève le réseau des réseaux. À l'instar des paradis fiscaux, il existe des paradis numériques où un malfaiteur peut agir ou héberger des serveurs et des contenus illicites en toute impunité. L'explosion du phénomène d'usurpation d'identité, depuis 2003, démontre que les criminels ont bien compris l'avantage qu'ils pouvaient obtenir non seulement des capacités d'« anonymisation » offertes par Internet, mais aussi de l'appropriation des fausses identités afin de ne pas être poursuivis ou tenus responsables d'actions criminelles ou terroristes.

Les technologies Internet et le cyberspace constituent donc une couche d'isolation protectrice pour les criminels.

La dématérialisation des transactions, les facilités de communication associées aux solutions de chiffrement, de stéganographie (2) et d'anonymat autorisent des liaisons entre criminels de différents pays sans contact physique, de manière flexible et sécurisée en toute impunité. Ainsi, ils peuvent s'organiser en équipe, planifier des actions illicites et les réaliser soit de manière classique, soit par le biais des nouvelles technologies. La couverture internationale du réseau Internet permet aux criminels d'agir au niveau mondial, à grande échelle et très rapidement, avec parfois un effet à retardement. (...)

La capacité de commettre des délits caché derrière un écran et à distance grâce aux réseaux permet l'ubiquité du criminel, dans le temps et dans l'espace. L'automatisation par logiciel des attaques contre des ressources informatiques mises en réseau (cyberattaques) autorise leur réalisation à grande échelle (notion de cyberépidémie) très rapidement. Ainsi, les moyens nécessaires pour réaliser un délit important peuvent être considérés comme faibles par rapport aux gains potentiels de la réalisation d'une attaque. Le retour sur investissement est alors optimal. Les différentes formes d'expression du crime informatique ont pour dénominateur commun qu'elles font courir relativement peu de risques à leur auteur et qu'elles engendrent des dommages potentiels bien supérieurs aux ressources nécessaires pour les réaliser.

2. Stéganographie (Steganography) : technique permettant de dissimuler une information dans une autre afin de la transmettre ou de la stocker clandestinement. Le marquage de document, le tatouage (watermarking), est une application de la stéganographie qui consiste à marquer une image de façon indélébile.

DOCUMENT N°5

Les diverses facettes du cyberspace criminologique

Stéphane LEMAN-LANGLAIS*, Marc OUIMET**

« Introduction », dossier « Le cybercrime » sous la direction de M. Ouimet et S. Leman-Langlois, *Criminologie*, © Les Presses de l'université de Montréal, printemps 2006, pp. 3, 5-6 (extraits).

Plusieurs journalistes, politiciens, policiers et experts en sécurité font aujourd'hui grand cas de cette nouvelle réalité nommée *cybercrime*. Les criminologues, pour leur part, ont jusqu'à maintenant été relativement discrets sur ce phénomène pourtant particulièrement révélateur aussi bien pour les études des politiques pénales, du passage à l'acte, de l'incrimination, de la réaction sociale que de la construction du crime.

Force est de constater qu'en importance absolue, l'influence du cybercrime, même dans sa définition la plus large, reste limitée sur le citoyen moyen (du moins pour l'instant). En soi, cette constatation pourrait s'appliquer à bien d'autres sphères marginales du phénomène criminel, qui, elles, sont pourtant couvertes d'une fébrilité sans cesse renouvelée par les chercheurs. L'autre facteur, sans doute plus déterminant, qui explique l'indifférence à l'égard du cybercrime est qu'il fait appel à des connaissances extrêmement éloignées de la criminologie. Tout simplement, il se trouve que peu de chercheurs sont intéressés à la fois au crime et à la compréhension d'une attaque DDOS (*Distributed Denial of Service*). (...)

En fait, nous pouvons approcher le cyberspace criminologique sous plusieurs aspects. Au plus simple, il s'agit effectivement d'un ensemble de nouveaux outils permettant de commettre des actes qui ressemblent à d'autres traditionnellement prescrits par le droit pénal ; par exemple, celui qui découvre un moyen de soutirer des numéros de cartes de crédit et qui s'en sert pour se procurer divers biens et services. Autre côté de la médaille, le cyberspace offre également de nouveaux outils de surveillance et de contrôle que l'État, l'entreprise privée, le groupe communautaire ou le citoyen peuvent utiliser à diverses fins. Un exemple de ce type de surveillance se retrouvant à l'intersection de tous ces intérêts est la publication des noms et adresses de prédateurs sexuels sur Internet, favorisant la manifestation de multiples formes de contrôle social.

Cela dit, nous pouvons également penser le cyberspace comme un contexte social, politique et individuel auquel les individus appartiennent, bien sûr à différents niveaux d'implication personnelle, mais dont l'augmentation à court terme est absolument garantie. Dans ce cybercontexte, les notions de sécurité, de liberté, de confiance, d'opportunité, de comportement, etc. prennent toutes des connotations différentes de celles qui ont cours dans la réalité sociale ordinaire :

- Cybercrime en tant qu'espace d'opportunités criminelles (outils nouveaux, cibles nouvelles) ;
- Cybercrime en tant qu'espace d'opportunités de contrôle (surveillance, information policière) ;
- Cybercrime en tant qu'espace virtuel d'(in)sécurité.

* Professeur à l'École de criminologie, chercheur au Centre international de criminologie comparée (CICC), Université de Montréal.
** Professeur, Département de criminologie, chercheur au Centre international de criminologie comparée (CICC), Université de Montréal.

DOCUMENT N°6

**L'évolution des cybercrimes :
données 2004**

CONSEIL DE L'EUROPE*

Criminalité organisée en Europe : la menace de la cybercriminalité. Rapport de situation 2004, Strasbourg, © Éditions du Conseil de l'Europe, 2006, pp. 236-237 (extrait).

Les statistiques officielles sur la cybercriminalité sont loin d'être réalistes dans la mesure où nombre d'infractions ne sont pas enregistrées du tout, où plusieurs cybercrimes ne sont pas enregistrés comme infractions séparées et où certains d'entre eux ne sont pas encore érigés en infractions pénales dans tous les pays. Néanmoins, il semblerait que les cybercrimes représentent la catégorie d'infractions augmentant le plus rapidement dans nombre de pays. Par exemple, une analyse des données collectées en Allemagne révèle que le nombre de délits informatiques enregistrés a énormément augmenté depuis 1987. La fraude au moyen de cartes de débit dotées d'un PIN obtenues illégalement, la fraude informatique et la fraude au moyen d'autorisations d'accès à des services de télécommunication représentent 90 % de l'ensemble des délits informatiques.

Les données collectées et les enquêtes effectuées dans différentes régions du monde en 2004 montrent notamment que :

- dans le monde entier, les attaques basées sur une usurpation frauduleuse d'identité et visant à obtenir des données à caractère personnel et financier ont considérablement augmenté pendant les huit premiers mois de 2004, causant des dommages importants ;
- 71 % des organisations privées et publiques interrogées en Australie et 64 % des sociétés interrogées aux États-Unis en 2004 ont signalé des incidents relatifs à des virus, vers et autres chevaux de Troie, ainsi que des vols d'informations ;
- 20 % des 494 sociétés interrogées aux États-Unis en 2004 ont fait l'objet de tentatives de sabotage et d'extorsion informatiques, notamment par le biais d'attaque DoS ;
- différentes enquêtes révèlent un accroissement des préjudices financiers imputables à la fraude informatique ;
- le nombre des sites web prônant le racisme, la haine et la violence aurait augmenté de 300 % entre 2000 et 2004. La plupart de ces sites sont hébergés sur des serveurs installés aux États-Unis, mais nombre d'entre eux sont en fait dirigés par des Européens ;
- concernant les infractions au droit d'auteur, la proportion de logiciels piratés dans les applications des utilisateurs des États membres du Conseil de l'Europe en 2003 varie entre 27 % en Autriche et en Suède, et 71 % en Bulgarie, 73 % en Roumanie, 87 % dans la Fédération de Russie et 91 % en Ukraine ;

* Programme Octopus.

• la pédopornographie représente l'un des marchés dont la croissance est la plus rapide. On estime qu'elle génère un chiffre d'affaires annuel de l'ordre de 20 milliards de dollars. Quelque 55 % du matériel serait originaire des États-Unis et 23 % de la Fédération de Russie. Des enquêtes menées en 2003 suggèrent que la pédopornographie représente 24 % des recherches d'image effectuées à l'aide d'une application Pair à Pair.

Les dispositifs nationaux

L'arsenal juridique français

Myriam QUÉMENER*

« Cybercriminalité : aspects stratégiques et juridiques », © *Défense nationale et sécurité collective*, 2008, pp. 26-34 (extraits).

Grâce à la loi n° 88-19 du 5 janvier 1988 dite « loi Godfrain », la France s'est dotée d'un dispositif répressif destiné à la lutte contre les manifestations du crime informatique visant à assurer la sécurité des systèmes d'information et à réprimer la fraude informatique. Les délits informatiques se trouvent désormais codifiés dans les articles 323-1 et suivants du code pénal, dans la section « des délits contre les systèmes de traitement automatisé de données ». Ils constituent le noyau dur de la criminalité informatique telle qu'elle était appréhendée initialement.

Les délits informatiques dans le code pénal

Ces dispositions répriment l'accès frauduleux dans un système informatique, et visent toute pénétration matérielle dans tout ou partie du système, comme par exemple l'intrusion par obtention des codes d'accès de façon irrégulière, les manipulations illicites, l'emploi d'un cheval de Troie. L'absence d'autorisation légale, administrative ou contractuelle pour accéder aux données est la seconde condition pour que l'infraction soit caractérisée. La loi n'a pas cependant précisé si l'accès illégal impliquait ou non la violation des dispositifs de sécurité. La seconde infraction est le maintien non autorisé dans un système, prévue par l'article 323-1 du code pénal, et présente un intérêt particulier par rapport à l'infraction précédente. Il s'agit, par exemple, de la personne qui a accédé régulièrement, mais qui s'est maintenue dans le système alors qu'elle n'était pas autorisée à le faire. Tel est le cas de la personne qui a accédé régulièrement à un service informatique et qui s'y maintient en envoyant des messages destinés à corrompre des clients.

Enfin, l'entrave volontaire au fonctionnement du système, prévue par l'article 323-2 du code pénal, est un délit spécifique, même s'il intervient postérieurement à des faits d'accès frauduleux. Les moyens utilisés pour porter atteinte aux systèmes sont multiples. Il peut s'agir de la destruction de matériel, de virus, de bombes logiques, de changement de code, d'envois massifs de messages dit *melbombing* (1). L'entrave peut être périodique ou permanente par perturbation du système. L'élément fondamental de l'infraction est constitué par l'action frauduleuse délibérée qui empêche un fonctionnement normal du système.

* Magistrat, substitut général à la cour d'appel de Versailles.
† Tribunal de grande instance de Nanterre, 1^{re} chambre, 8 juin 2006, site forum des droits de l'internet (www.foruminternet.org).

La loi réprime enfin la participation à un groupe de personnes en vue de préparer une ou plusieurs infractions informatiques évoquées ci-dessus, transposant ainsi l'infraction d'association de malfaiteurs au monde des réseaux numériques. Cette incrimination est souvent retenue pour sanctionner des actes de complicité plutôt que pour réprimer les actes préparatoires au délit. Afin d'établir l'infraction, il convient de rassembler des éléments objectifs, comme l'échange de matériels, de codes d'accès, de logiciels, ce qui est parfois complexe en pratique. La tentative de ces infractions est punissable, à l'exception du délit d'entente (2), et les personnes morales peuvent être déclarées responsables (article 323-6 du CP).

Les articles 323-1 et suivants du code pénal répriment, au chapitre des atteintes aux systèmes de traitement automatisé des données, le fait d'accéder ou de se maintenir dans un système de traitement automatisé, ou d'en modifier le contenu, d'en entraver le fonctionnement ou d'y introduire des données, ou d'en modifier le fonctionnement. L'association de malfaiteurs, définie comme la participation à un groupement formé ou à une entente établie, en vue de la préparation, caractérisée par un ou plusieurs faits matériels d'une ou plusieurs infractions, est spécialement incriminée lorsqu'elle est constituée en vue de commettre des atteintes aux systèmes de traitement automatisé des données.

La loi du 15 novembre 2001 relative à la sécurité quotidienne

Force est de constater que l'émergence d'actions et d'attentats terroristes a accéléré les évolutions législatives concernant les réseaux numériques et l'Internet. Ainsi, la loi n° 2001-1062 du 15 novembre 2001 a posé le principe de la conservation pour une durée d'un an des données de connexion des abonnés par les opérateurs de téléphonie fixe et mobile et aux fournisseurs d'accès à Internet pour les besoins d'une procédure pénale (3).

Le texte pose un principe, celui de l'effacement des données, accompagné de trois exceptions autorisant la conservation des données de connexion, à savoir la recherche, la constatation et la poursuite des infractions pénales, pour les besoins de facturation des entreprises et pour des questions de sécurité informatique.

La loi permet aussi aux autorités judiciaires de disposer désormais de moyens renforcés de l'État couverts par le secret de la défense nationale aux fins de procéder à un décryptage des données. Tel est le cas lorsqu'un moyen de cryptologie aurait été utilisé pour commettre un crime ou un délit en matière de terrorisme, par exemple.

Cette loi a créé un observatoire de la sécurité des cartes de paiement afin de cerner ce contentieux de masse que représente notamment la contrefaçon de cartes bancaires.

2 Article 323-7
du code pénal
3 Article 323-7
du code pénal.

La loi du 21 juin 2004 pour la confiance dans l'économie numérique

Ce texte fondateur met en place un statut juridique de l'Internet et vise à sécuriser son usage en clarifiant le régime de responsabilités des prestataires de service, tout en mettant en œuvre une protection efficace pour les internautes.

Les prestataires techniques, aux termes de l'article 6 de la loi, n'ont pas d'obligation générale de surveillance et de recherche d'activités illicites, notamment en ce qui concerne les contenus qu'ils hébergent, transportent ou stockent. Ainsi, le statut « d'hébergeur » comporte un régime de responsabilité moins étendu au regard des contenus hébergés que celui « d'éditeur ».

En revanche, ils ont une obligation spéciale de concourir à la lutte contre l'apologie des crimes contre l'humanité, l'incitation à la haine, la pornographie infantile, l'incitation à la violence, les atteintes à la dignité humaine. À cette fin, ils doivent mettre en place un dispositif technique de dénonciation de ce type de données et informer promptement les autorités publiques compétentes de toutes activités illicites portées à leur connaissance. Ils doivent en outre rendre publics les moyens consacrés à la lutte contre ces activités. Le rapport de l'Assemblée nationale, publié récemment (4), préconise même d'élargir cette obligation de publicité aux atteintes aux intérêts privés, tels la diffamation, les droits d'auteur et la contrefaçon.

Cette loi sécurise les échanges et amplifie les moyens de lutte contre la cybercriminalité en réprimant, par exemple, l'importation, la détention, l'offre, la cession ou la mise à disposition sans motif légitime d'éléments d'intrusion, comme des virus. Elle met aussi en place un cadre pour l'économie numérique, comme la délimitation de l'e-commerce, la responsabilité des commerçants en ligne, l'encadrement juridique des instruments de commerce électronique. Enfin, elle améliore, tout en l'encadrant, l'accès des personnes privées aux moyens de cryptologie.

La loi du 23 janvier 2006 relative à la lutte contre le terrorisme

Ce texte relatif à la lutte contre le terrorisme et portant dispositions diverses sur la sécurité et les contrôles frontaliers a pris en compte l'importance du réseau Internet comme vecteur d'échange d'informations à caractère terroriste.

La loi n° 2006-64 a complété la liste des personnes soumises à l'obligation de conservation et de communication à la justice des données techniques, tels les cybercafés et les bornes wifi (5), qui sont désormais assimilés à des opérateurs de communications électroniques. Cette disposition a ainsi pour objectif de permettre aux services de police d'identifier les clients d'un cybercafé et de cerner les connexions, car il

4 Consultable sur le site www.juriscor.net
5 L'article 5 de cette loi, portant création de l'article L.34-1-1 du code des postes et des télécommunications, permet l'assimilation des cybercafés à des opérateurs de téléphonie.

a été souvent constaté que les terroristes échangeaient avant de commettre des attentats.

Le décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques en a précisé la liste. Cependant, en pratique, les services de lutte contre le terrorisme déplorent l'absence d'obligation d'identification des clients ayant recours à ces services, qui constitue une réelle limite à l'utilité de la disposition. Il serait à cet égard peut-être pertinent de s'inspirer de la législation italienne qui exige la sollicitation d'une autorisation préalable ainsi que l'identification de l'ensemble des clients (6).

La loi a créé un dispositif d'accès de certains agents des services chargés de la prévention du terrorisme aux données conservées par les opérateurs de communications électroniques et les hébergeurs de site Internet (7).

La loi du 1^{er} août 2006 relative au droit d'auteur et aux droits voisins (loi « DADVS »)

Transposition de la directive du 22 mai 2001 relative au droit d'auteur, ce texte vise à préserver les droits des créateurs. Sur le plan de la cyberdélinquance, trois axes sont à signaler.

En premier lieu, l'offre de moyens illicites de mise à disposition du public d'œuvres ou objets protégés est réprimée. Les éditeurs et les distributeurs de logiciels dédiés ou utilisés dans ce but sont passibles du délit de contrefaçon. Les logiciels d'échange de données ou de fichiers configurés spécifiquement pour faire circuler des fichiers contenant des mesures techniques de protection sont exclus de cette catégorie. Les peines complémentaires sont la confiscation des recettes tirées de l'exploitation du logiciel litigieux, la publication du jugement, la fermeture de l'établissement ou encore l'interdiction d'exercer l'activité d'édition ou de distribution de logiciels.

En second lieu, la mise à disposition du public d'œuvres en violation des droits d'auteur constitue une forme illicite de représentation ou de communication au public, punie par le délit de contrefaçon. Le fait que cette mise à disposition illicite précède la mise à disposition officielle du public en France, violant ainsi le principe de « la chronologie des médias » issu de la loi n° 82-652 du 29 juillet 1982 (8) sur la communication audiovisuelle, est considéré comme une circonstance aggravante. Les internautes qui utilisent des logiciels *peer to peer* les obligeant à mettre à disposition des autres usagers les fichiers lors du téléchargement (9) sont exclus de cette catégorie.

Enfin, les internautes effectuant des téléchargements illicites font l'objet par leurs fournisseurs d'accès à Internet (FAI) d'une mise en garde préalable et de messages de sensibilisation. Le téléchargement constituant une reproduction d'une œuvre en fraude des droits de son

6 Voir sur ce point le rapport de la commission des lois sur la mise en application de la loi n° 2006-64 du 23 janvier 2006 (www.legifrance.gouv.fr).
7 Disposition applicable suite à la parution du décret n° 2006-1651 du 22 décembre 2006 pris pour l'application du I de l'article 6 de la loi n° 2006-64 du 23 janvier 2006 qui précise que les demandes de réquisitions administratives doivent être faites par des agents habilités.
8 JO du 30 juillet 1982 (www.legifrance.gouv.fr).
9 Ce qui est le cas, par exemple, du logiciel *emule*.

auteur, ce qui est constitutif d'un acte de contrefaçon, est sanctionné pénalement. Des peines exclusivement pécuniaires sont prévues ici, toujours avec une gradation : par exemple, sont pris en compte la réciproque, le nombre ou le volume élevé des téléchargements illicites, l'antériorité du téléchargement à la diffusion commerciale officielle, la mise à disposition automatique durant le téléchargement.

La jurisprudence s'est prononcée à de nombreuses reprises concernant les utilisateurs de *peer to peer* poursuivis pour reproduction ou diffusion non autorisée de programme, vidéogramme ou phonogramme, contrefaçon par édition ou reproduction d'une œuvre de l'esprit au mépris des droits d'auteur. Dans ce cas, l'exception de copie privée est expressément écartée, ce qui est logique, car cette dernière ne vise qu'un usage privé, alors que, dans l'hypothèse du téléchargement illicite, il s'agit d'une copie faite pour autrui.

Un échelonnement de la sanction pénale est officialisé entre la personne qui aura conçu et diffusé un logiciel permettant des échanges illicites, et dont il tirera un revenu conséquent, la personne qui mettra en ligne un volume très important de fichiers illégaux et la personne qui, très ponctuellement, téléchargera une toute petite quantité de ces fichiers. Même si cette gradation avait déjà cours de façon informelle, cela permettra d'éviter l'insécurité juridique liée aux différentes méthodes de calcul de la sanction pécuniaire. Les internautes ne doivent pas oublier qu'à côté des sanctions pénales, la peine la plus lourde se situe souvent au niveau de la condamnation civile. En effet, le montant des dommages et intérêts réclamés par les titulaires de droit peut atteindre parfois plusieurs centaines de milliers d'euros.

Enfin, il convient de souligner qu'en dépit de la promulgation de la loi n° 2006-961 du 1^{er} août 2006 relative au droit d'auteur et aux droits voisins, la réflexion afin de trouver des solutions au problème du téléchargement illicite, complémentaire de la répression de la contrefaçon, n'est certainement pas en l'état aboutie. En effet, les réponses pénales semblent quelque peu disproportionnées ; d'ailleurs, les tribunaux n'ont jamais prononcé de peines d'emprisonnement ferme et les amendes sont généralement faibles et assorties du sursis.

Les lois du 5 mars 2007 relatives à la prévention de la délinquance et réformant la protection de l'enfance

Tenant compte de l'utilisation croissante par les jeunes des nouvelles technologies, en particulier d'Internet, la loi relative à la prévention de la délinquance vise à améliorer leur protection contre des utilisations délictueuses. Par exemple, cette loi a prévu la signalisation de l'interdiction aux mineurs des supports vidéo à contenu violent, emportant l'interdiction de louer, de proposer ou de vendre ceux-ci à des mineurs.

Par ailleurs, l'utilisation d'un moyen de communication électronique pour faire une proposition sexuelle à un mineur constitue une

infraction spécifique, la peine étant majorée lorsque cet agissement est suivi d'une rencontre. Sans sombrer dans l'inventaire, il faut comprendre que la norme pénale s'adapte constamment aux évolutions non seulement techniques mais aussi comportementales. Ainsi, la loi a créé un nouveau délit, le *happy slapping*, qui réprime les actes d'enregistrement et de diffusion d'images d'agressions, afin de répondre à l'essor de ce nouveau phénomène de violence gratuite.

Dans le domaine du renforcement des moyens d'investigation, ce texte donne l'autorisation aux policiers et aux gendarmes d'infiltrer les réseaux numériques tels Internet pour repérer les délinquants et les interpellier lors d'enquêtes dans le domaine de la corruption de mineurs et de la pédopornographie, mais aussi en matière de traite des êtres humains, du recours à la prostitution de mineurs et de proxénétisme. Dans ce cadre, sous réserve que leurs actes ne constituent pas une incitation à commettre les infractions, les policiers et gendarmes peuvent devenir des « cyber-patrouilles », c'est-à-dire qu'ils peuvent participer aux échanges électroniques sous un pseudonyme et entrer en contact avec les auteurs d'infractions.

Enfin, la loi portant réforme de la protection de l'enfance crée un article 227-23, alinéa 5 du code pénal qui réprime la consultation habituelle d'images pédopornographiques. La France poursuit son action en la matière et un plan d'action a été lancé dernièrement par le gouvernement qui constitue une nouvelle étape de la lutte contre la cybercriminalité. Une charte de bonnes pratiques avec les opérateurs de communications électroniques va être élaborée. Par ailleurs, de nouvelles incriminations sont prévues dans le cadre de la prochaine loi d'orientation et de programmation pour la sécurité intérieure (Lopsi), comme l'usurpation d'identité par Internet.

La coopération internationale : une nécessité

La coordination de la lutte contre la cybercriminalité dans l'Union européenne

COMMISSION DES COMMUNAUTÉS EUROPÉENNES

« Vers une politique générale en matière de lutte contre la cybercriminalité », communication de la Commission au Parlement européen, au Conseil et au Comité des régions, Bruxelles, 22 mai 2007, COM (2007) 267 final (extraits).

La Commission lance une initiative en faveur d'une politique générale visant à améliorer la coordination de la lutte contre la cybercriminalité à l'échelle européenne et internationale.

(...) L'initiative sera axée sur deux dimensions de cette lutte, la répression et le droit pénal. La politique qui en résultera viendra compléter d'autres mesures prises par l'Union pour améliorer la sécurité dans le cyberspace en général. Elle portera sur les éléments suivants : l'amélioration de la coopération opérationnelle entre les services répressifs, l'amélioration de la coopération et de la coordination politiques entre les États membres, la coopération politique et juridique avec les pays tiers, la sensibilisation, la formation, la recherche, le renforcement du dialogue avec l'industrie et d'éventuelles mesures législatives.

La politique relative à la lutte contre la cybercriminalité et aux poursuites engagées contre celle-ci sera définie et mise en œuvre dans le plein respect des droits fondamentaux, notamment de la liberté d'expression, du respect de la vie privée et familiale et de la protection des données à caractère personnel. Toute mesure législative prise dans le cadre de cette politique sera tout d'abord examinée au regard de sa compatibilité avec ces droits, notamment ceux consacrés par la charte des droits fondamentaux de l'UE. (...)

Instruments et mesures adoptés au niveau de l'UE

La présente communication relative à la politique en matière de cybercriminalité consolide et développe la communication de 2001 intitulée « Créer une société de l'information plus sûre en renforçant la

sécurité des infrastructures de l'information et en luttant contre la cybercriminalité » (1) (ci-après dénommée : la communication de 2001). Celle-ci proposait des dispositions législatives pertinentes, de fond et de procédure, pour réprimer les activités criminelles nationales et transnationales. Plusieurs propositions importantes en ont résulté, notamment celle qui a donné lieu à la décision-cadre 2005/222/JAI relative aux **attaques visant les systèmes d'information** (2). Dans ce contexte, il convient également de noter que d'autres instruments législatifs, plus généraux, ont été adoptés qui portent aussi sur des aspects de la lutte contre la cybercriminalité, tels que la décision-cadre 2001/413/JAI concernant la **lutte contre la fraude et la contrefaçon des moyens de paiement** autres que les espèces (3).

La décision-cadre 2004/68/JAI relative à la **lutte contre l'exploitation sexuelle des enfants et la pédopornographie** (4) illustre bien l'attention particulière accordée par la Commission à la protection des enfants, notamment contre toutes les formes de contenus illicites ayant trait à la violence sexuelle exercée contre les enfants qui sont publiés par l'intermédiaire de systèmes d'information, une priorité horizontale qui sera maintenue à l'avenir.

Pour relever les défis de sécurité qui se posent à la société de l'information, la Communauté européenne a élaboré une triple approche à l'égard de la sécurité des réseaux et de l'information : des mesures spécifiques relatives à la sécurité des réseaux et de l'information, le cadre réglementaire pour les communications électroniques et la lutte contre la cybercriminalité. Bien que ces trois volets puissent, dans une certaine mesure, être élaborés séparément, leurs nombreuses interdépendances plaident pour une coordination étroite. Dans le domaine connexe de la **sécurité des réseaux et de l'information**, une communication de la Commission, intitulée « Sécurité des réseaux et de l'information : proposition pour une approche politique européenne » (5), a été adoptée en 2001, parallèlement à celle consacrée à la cybercriminalité la même année. La directive 2002/58/CE « Vie privée et communications électroniques » fait obligation aux fournisseurs de services de communications électroniques accessibles au public de garantir la sécurité de leurs services. Elle contient aussi des dispositions contre le *pourriel* (*spam*) et les *espiogiciels* (*spyware*). La politique relative à la sécurité des réseaux et de l'information a été complétée depuis par plusieurs mesures, tout récemment dans la communication intitulée « Une stratégie pour une société de l'information sûre » (6), qui expose une stratégie revitalisée et définit le cadre permettant d'approfondir et de préciser une approche cohérente en matière de sécurité des réseaux et de l'information, ainsi que dans la communication sur la lutte contre le *pourriel*, les *espiogiciels* et les *logiciels malveillants* (7), et par la création en 2004 de l'Agence européenne chargée de la sécurité des réseaux et de l'information (8).

1 COM (2000) 890 du 26.1.2001.
 2 JO L 69 du 16.3.2005, p. 67.
 3 JO L 149 du 2.6.2001, p. 1.
 4 JO L 13 du 20.1.2004, p. 44.
 5 COM (2001) 298.
 6 COM (2004) 251.
 7 COM (2006) 688.
 8 Règlement (CE) n° 460/2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information (JO L 77 du 13.3.2004, p. 1).

L'Agence a pour principal objectif d'acquérir des compétences spécialisées pour encourager la coopération entre les acteurs des secteurs public et privé, ainsi que de prêter assistance à la Commission et aux États membres. Les résultats des recherches menées dans le domaine technologique pour sécuriser les systèmes d'information joueront également un rôle majeur dans la lutte contre la cybercriminalité. Par conséquent, les technologies de l'information et de la communication ainsi que la sécurité figurent parmi les objectifs du septième programme-cadre de recherche de l'UE, qui sera opérationnel de 2007 à 2013. La révision du cadre réglementaire pour les communications électroniques pourrait donner lieu à des modifications destinées à renforcer l'efficacité des dispositions relatives à la sécurité figurant dans la directive « Vie privée et communications électroniques » et la directive 2002/22/CE « Service universel » (9). (...)

Renforcer la coopération opérationnelle entre les services répressifs et les efforts de formation

L'absence ou la sous-utilisation de structures immédiates pour la coopération opérationnelle transfrontalière demeure une faiblesse importante du domaine de la justice, de la liberté et de la sécurité. Dans les affaires urgentes de cybercriminalité, l'entraide traditionnelle s'avère lente et inefficace, et la mise en place de nouvelles structures de coopération n'est pas encore satisfaisante. Si les services judiciaires et répressifs nationaux coopèrent étroitement en Europe par l'intermédiaire d'Europol, d'Eurojust et d'autres structures, il y a manifestement lieu de renforcer et de clarifier les responsabilités. Les consultations lancées par la Commission indiquent que l'utilisation de ces canaux fondamentaux n'est pas optimale. L'approche européenne, davantage coordonnée, doit être tant opérationnelle que stratégique et englober aussi l'échange d'informations et de bonnes pratiques.

Dans un avenir proche, la Commission insistera particulièrement sur les besoins de formation. Il est avéré que les évolutions technologiques requièrent une formation continue des services répressifs et judiciaires aux questions touchant à la cybercriminalité. Un soutien financier renforcé et mieux coordonné de l'UE est donc envisagé en faveur de programmes de formation multinationaux. En outre, dans le cadre d'une coopération étroite avec les États membres et d'autres organes compétents tels qu'Europol, Eurojust, le Collège européen de police (CEPOL) et le Réseau européen de formation judiciaire (REFJ), la Commission s'efforcera de coordonner et de relier au niveau de l'Union tous les programmes de formation pertinents. (...)

9 COM (2006) 334,
SEC (2006) 816,
SEC (2006) 817.

Renforcer le dialogue avec l'industrie

Les secteurs privé et public ont tous deux intérêt à élaborer conjointement des méthodes de détection et de prévention des dommages causés par les activités criminelles. Une participation commune des secteurs privé et public, fondée sur la confiance mutuelle et un même objectif, celui de réduire les dommages, promet d'être un moyen efficace pour accroître la sécurité, également dans le cadre de la lutte contre la cybercriminalité. (...)

Des opérateurs privés contrôlent en grande partie l'évolution des technologies de l'information et des systèmes de communications électroniques modernes. Des entreprises privées évaluent les menaces, définissent des programmes de lutte contre la criminalité et élaborent des solutions techniques pour prévenir celle-ci. L'industrie s'est montrée très encline à aider les pouvoirs publics à combattre la cybercriminalité, notamment en ce qui concerne la lutte contre la pédopornographie (10) et d'autres types de contenus illicites sur Internet.

Une autre question concerne le manque apparent d'échanges d'informations, de compétences spécialisées et de bonnes pratiques entre les secteurs public et privé. Pour protéger des modèles et des secrets d'entreprise, les opérateurs privés rechignent souvent – la loi ne les y obligeant pas clairement – à communiquer aux services répressifs des informations pertinentes relatives à la fréquence des délits. Or, ces informations peuvent être indispensables pour que les pouvoirs publics puissent élaborer une politique de lutte contre la criminalité qui soit efficace et appropriée. Les moyens d'améliorer les échanges d'information intersectoriels seront envisagés également au regard des règles en vigueur en matière de protection des données à caractère personnel.

La Commission joue déjà un rôle important dans diverses structures, associant les secteurs public et privé, qui luttent contre la cybercriminalité, telles que le groupe d'experts en matière de prévention de la fraude (11). Elle est persuadée qu'une politique générale efficace pour combattre la cybercriminalité doit également comprendre une stratégie de coopération entre les acteurs des secteurs public et privé, y compris les organisations de la société civile.

10 Un exemple de coopération dans ce domaine est la collaboration entre des services répressifs et des sociétés émettrices de cartes de crédit, dans le cadre de laquelle celles-ci ont aidé les services de police à localiser des acheteurs de pédopornographie en ligne.

11 Voir le site http://ec.europa.eu/internal_market/payments/fraud/index_fr.htm

Un nouveau défi pour les systèmes de justice pénale

CONSEIL DE L'EUROPE

Criminalité organisée en Europe. La menace de la cybercriminalité, rapport de situation 2004, Strasbourg, © Éditions du Conseil de l'Europe, pp. 225-228 (extraits).

Les nouveaux problèmes posés par la cybercriminalité au système de justice pénale ne sont pas uniquement dus aux difficultés pratiques inhérentes à la lutte contre la délinquance informatique. Le principal facteur de complication découle en fait de la complète opposition entre les nouvelles caractéristiques de la cybercriminalité et celles du droit traditionnel.

Inadéquation entre les systèmes de droit pénal et la délinquance informatique

Sur la base de l'analyse des caractéristiques de la délinquance informatique à laquelle nous avons procédé dans la section précédente, il est notamment possible d'évoquer les principales incompatibilités suivantes :

- le droit pénal traditionnel vise surtout à protéger des biens tangibles clairement définis contre des attaques menées par des hommes. En revanche, les délits informatiques violent fréquemment de nouvelles valeurs intangibles dépendant d'un équilibre délicat d'intérêts et se prêtant peu à une définition par le biais de termes et de dispositions généraux. Des exemples de cet équilibre difficile se retrouvent dans le droit de la propriété intellectuelle (compromis entre les intérêts économiques des créateurs et les demandes d'information légitimes de la société), le droit à la vie privée (compromis entre la protection de la vie privée et la liberté de traiter l'information), ainsi que dans la réglementation des contenus nocifs (compromis entre la protection des mineurs, des minorités et des groupes raciaux et le droit à la liberté de l'information des adultes) ;
- les systèmes traditionnels de droit pénal se fondent sur l'idée de la souveraineté nationale, de sorte que la portée directe des décisions judiciaires qu'ils génèrent est limitée au territoire national du pays concerné. Néanmoins, Internet est un média véritablement universel. Les aspects géographiques – tels que l'emplacement où l'information est physiquement stockée – revêtent une importance mineure. Les données transférées transitent par différents pays et régions en ignorant les frontières et les lignes de démarcation ;

- les systèmes traditionnels de droit pénal sont lents : les décisions prises par la police doivent fréquemment être confirmées par un juge ; souvent, l'accusé a le droit d'être entendu et d'interjeter appel contre une décision judiciaire le concernant ; quant aux procédures transnationales, elles sont extrêmement formalistes. En revanche, Internet est un système très rapide : alors que le transfert de décisions judiciaires nationales prend des semaines ou des mois, les données informatiques peuvent être expédiées dans un pays étranger en quelques millisecondes. La vitesse du processus de transfert et cette interaction multinationale posent un défi à tous les systèmes et institutions nationaux de droit pénal. Les données peuvent être effacées ou altérées en quelques millisecondes dans n'importe quel point du globe ; les fichiers de consignation sont souvent conservés pendant un temps limité et les données relatives au trafic – révélant l'origine d'une chaîne de communication – pendant une courte période. Cette tension peut avoir des conséquences désastreuses sur l'efficacité des enquêtes. Alors que la police commence à vérifier le contenu d'un système dans un local A, l'auteur de l'infraction peut facilement effacer les données pertinentes sur les unités de stockage depuis un local B. Ou bien, lorsque la police reçoit les données relatives au trafic d'un fournisseur d'accès Internet, le fournisseur suivant dans la chaîne de communication faisant l'objet de l'enquête a déjà effacé les données nécessaires à l'identification de l'expéditeur ;

- dans une procédure pénale, les auteurs du délit doivent être identifiés et de solides preuves de leur culpabilité doivent être produites. Ces exigences compliquent les poursuites intentées contre les auteurs de délits informatiques commis contre des réseaux dans la mesure, surtout, où Internet est difficile à contrôler et garantit – du moins aux utilisateurs avertis – un niveau élevé d'anonymat. Les réseaux informatiques internationaux (dotés de relais de messagerie anonymes ou de dispositifs d'accès libre aux fournisseurs d'accès Internet) assurent aux contrevenants un anonymat qui ne pourra être levé que si tous les pays que la communication traverse décident de coopérer. En outre, les systèmes informatiques et de communication sont de plus en plus livrés avec de puissants logiciels de cryptage et la possibilité de dissimuler des données. Aujourd'hui, des logiciels standard assurent ces deux fonctions en dissimulant par exemple les données dans des images (stéganographie). L'obtention des informations requises pour entamer des poursuites avec des chances de succès dans ce domaine est particulièrement difficile, dans la mesure où nombre de juridictions limitent l'accès aux informations sensibles relatives aux utilisateurs (indispensables pour identifier les contrevenants). Toute proposition visant à limiter cet anonymat attire automatiquement les foudres des inconditionnels de la protection des données et du secret des télécommunications.

Quelles perspectives ?

L'analyse de la section précédente et la description de l'inadéquation entre le droit pénal traditionnel et la délinquance informatique soulignent la difficulté de combattre efficacement cette délinquance et expliquent pourquoi la cybercriminalité, en particulier, est un défi majeur pour ce système juridique.

Néanmoins, ces observations générales suggèrent aussi des solutions futures aux systèmes de droit pénal traditionnels. Afin de relever les nouveaux défis posés par la cybercriminalité, le droit pénal doit s'adapter aux nouveaux phénomènes :

- le droit pénal matériel doit non seulement couvrir les nouvelles formes d'attaques contre les valeurs corporelles traditionnelles, mais aussi protéger les nouvelles valeurs (surtout intangibles) de la société de l'information contemporaine et, plus spécialement, prendre en compte les questions de droit civil associées à la protection du droit d'auteur et des données, ainsi que des mineurs. Certes, depuis quelques années, des institutions internationales et supranationales, ainsi que des législateurs nationaux, tentent sérieusement de réformer le droit matériel afin de répondre aux nouveaux défis posés par le cyberspace ; cependant, force est de constater la survivance de lacunes législatives importantes dans ce domaine, surtout en ce qui concerne l'incrimination du recours aux outils de piraterie, la protection des mineurs, la lutte contre la fraude et le courrier électronique non sollicité et la sauvegarde des systèmes de gestion des droits numériques ;
- le droit procédural et les services répressifs doivent s'attaquer aux problèmes inhérents à l'anonymat, au manque de preuves et au besoin de disposer de nouveaux pouvoirs de coercition et de nouveaux outils d'enquête informatique. Nombreux sont les praticiens qui considèrent cette bataille perdue d'avance. Toutefois, ce constat semble beaucoup trop pessimiste, dans la mesure où la technologie de l'information crée des problèmes supplémentaires en matière de répression des délits, mais aussi de nouvelles opportunités. Cette technologie peut être un puissant instrument non seulement pour les criminels, mais aussi pour les services de police et le ministère public qui peuvent l'exploiter pour élaborer de nouveaux outils et stratégies de surveillance. De sorte que le défi, à l'avenir, consistera à construire et à utiliser ces nouveaux instruments tout en conciliant les besoins d'une répression efficace et la protection de la vie privée ;
- les accords de coopération internationaux doivent trouver de nouvelles solutions pour garantir une coopération entre les différentes juridictions et leurs autorités nationales de poursuite. Le contraste entre la nature universelle de la délinquance informatique et la portée purement nationale du droit pénal rend la coopération entre ministères publics indispensable. Les traités internationaux d'entraide judiciaire devraient donc autoriser les mêmes actions que le droit procédural national ;
- le droit pénal international doit apporter de nouvelles réponses à la question de savoir comment appliquer le droit pénal au cyberspace virtuel. Bien que les éléments corporels des systèmes et réseaux informatiques se situent sur le territoire d'États, les règles traditionnelles d'application territoriale du droit ne suffisent pas en l'espèce. En outre, il conviendrait d'élaborer un droit supranational, d'harmoniser les droits nationaux, d'améliorer les procédures de coopération et de forger de nouvelles règles en matière d'application internationale du droit pénal pour répondre aux nouveaux défis mondiaux posés par la cybercriminalité.

La ratification par de nombreux pays de la Convention du Conseil de l'Europe sur la cybercriminalité et de son protocole, ainsi que la mise en œuvre d'autres instruments et recommandations internationaux consacrés à la délinquance informatique constitueraient un pas décisif vers l'acceptation de ces défis.

LAP.

Partiel
2^e semestre

Jeu. 31/13/11

Note de Synthèse

P.1

M. LE MERCIER -

MINISTÈRE DES TRANSPORTS, DE L'ÉQUIPEMENT

DU TOURISME ET DE LA MER

**CONCOURS EXTERNE
POUR LE RECRUTEMENT
D'INSPECTRICES ET D'INSPECTEURS DU PERMIS
DE CONDUIRE ET DE LA SÉCURITÉ ROUTIÈRE**

SESSION 2007

ÉPREUVE N° 1

Rédaction d'une note de synthèse

Rédaction d'une note de synthèse à partir d'un dossier portant sur un sujet d'ordre général permettant de vérifier l'aptitude à la compréhension des textes ainsi que les capacités de synthèse de rédaction des candidats

(durée : trois heures ; coefficient 2)

Ce sujet comporte 39 pages, y compris celle-ci.

Rédaction d'une note de synthèse

(durée : trois heures ; coefficient 2)

SUJET

A l'aide des documents joints, vous rédigerez une note sur la lutte contre le tabagisme. En exposant les objectifs et les mesures prises ou envisagées, notamment en terme de santé publique, vous montrerez les perspectives de réussite de la politique dans ce domaine et les freins à sa mise en oeuvre.

Votre devoir ne devra pas excéder 6 pages

DOCUMENTS JOINTS

Document 1	Loi 91-32 du 10 janvier 1991 - JO du 21 janvier 1991	1 page
Document 2	Décret no 92-478 du 29 mai 1992 fixant les conditions d'application de l'interdiction de fumer dans les lieux affectés à un usage collectif et modifiant le code de la santé publique	3 pages
Document 3	Comité français d'éducation pour la santé - La santé en chiffres : le tabac - Décembre 1999	10 pages
Document 4	Le Parc des expositions de la Ville de Paris condamné pour non application de la loi Evin - Communication du Centre National contre la tabagisme - 22 février 2005	1 page
Document 5	Observatoire français des Drogues et de la toxicomanie - Bilan tabagique en milieu scolaire - 31 mars 2004	2 pages
Document 6	Article Le Monde : Les ventes de cigarettes ont augmenté au premier semestre 2006, la dissuasion par les prix a échoué - 17 août 2006	1 page

CONCOURS EXTERNE IPCSR SESSION 2007

Document 7	Site IEP-Toulouse : article point européen : fin de la tolérance en Europe pour les fumeurs - 20 novembre 2006	2 pages
Document 8	Mission interministérielle de lutte contre la drogue et la toxicomanie - Janvier 2006 - Le tabac et la loi	2 pages
Document 9	Article Le Monde 27/09/06: De l'efficacité d'interdire	2 pages
Document 10	Site IEP-Toulouse : interview de patrons de bar - 20 octobre 2006	2 pages
Document 11	Décret n° 2006-1386 du 15 novembre 2006 fixant les conditions d'application de l'interdiction de fumer dans les lieux affectés à un usage collectif - JO du 16 novembre 2006	4 pages
Document 12	site www.place-publique.fr - Le site des initiatives citoyennes - Octobre 2006 ; contre l'interdiction de fumer	1 page
Document 13	Extrait Rapport ASPECT (analyse des sciences et des politiques européennes contre le tabagisme) de la Commission européenne sur le lutte contre le tabac au sein de l'Union - 2002	5 pages

LOIS

LOI n° 91-32 du 10 janvier 1991 relative à la lutte contre le tabagisme et l'alcoolisme (1)

NOR : SP5X9000097L

L'Assemblée nationale et le Sénat ont adopté,
Vu la décision du Conseil constitutionnel n° 90-283 DC en date du 8 janvier 1991,

Le Président de la République promulgue la loi dont la teneur suit :

Art. 1^{er}. - A compter du 1^{er} janvier 1992, il est interdit de prendre en compte le prix du tabac pour le calcul des indices de prix à la consommation, publiés par les administrations de l'Etat, et notamment l'Institut national de la statistique et des études économiques.

Art. 2. - L'article L. 192 du code de la santé publique est complété par un alinéa ainsi rédigé :

« Ils reçoivent à cette occasion par le médecin scolaire une information concernant les causes, les conséquences et les moyens de traitement et de lutte contre le tabagisme, l'alcoolisme et la toxicomanie. »

TITRE I^{er}

DISPOSITIONS RELATIVES À LA LUTTE CONTRE LE TABAGISME

Art. 3. - I. - A compter du 1^{er} janvier 1993, l'article 2 de la loi n° 76-616 du 9 juillet 1976 relative à la lutte contre le tabagisme est ainsi rédigé :

« Art. 2. - Toute propagande ou publicité, directe ou indirecte, en faveur du tabac ou des produits du tabac ainsi que toute distribution gratuite sont interdites.

« Ces dispositions ne s'appliquent pas aux enseignes des débits de tabac, ni aux affichettes disposées à l'intérieur de ces établissements, non visibles de l'extérieur, à condition que ces enseignes ou ces affichettes soient conformes à des caractéristiques définies par arrêté interministériel.

« Toute opération de parrainage est interdite lorsqu'elle a pour objet ou pour effet la propagande ou la publicité directe ou indirecte en faveur du tabac ou des produits du tabac. »

II. - Jusqu'au 1^{er} janvier 1993, les dispositions actuelles de l'article 2 de la loi n° 76-616 du 9 juillet 1976 demeurent en vigueur sous réserve de la modification suivante : après les mots : « de propagande et de publicité » sont insérés les mots : « , directe ou indirecte, ».

Art. 4. - Les articles 1^{er}, 3, 9, 12, 16 et 18 de la loi n° 76-616 du 9 juillet 1976 précitée sont ainsi rédigés :

« Art. 1^{er}. - Sont considérés comme produits du tabac les produits destinés à être fumés, prisés, mâchés ou sucés, dès lors qu'ils sont, même partiellement, constitués de tabac, ainsi que les produits destinés à être fumés même s'ils ne contiennent pas de tabac, au sens du troisième alinéa (2^o) de l'article 564 *decies* du code général des impôts. »

« Art. 3. - Est considérée comme propagande ou publicité indirecte toute propagande ou publicité en faveur d'un organisme, d'un service, d'une activité, d'un produit ou d'un article autre que le tabac ou un produit du tabac lorsque, par son graphisme, sa présentation, l'utilisation d'une marque, d'un emblème publicitaire ou de tout autre signe distinctif, elle rappelle le tabac ou un produit du tabac.

« Toutefois, ces dispositions ne sont pas applicables à la propagande ou à la publicité en faveur d'un produit autre que le tabac ou un produit du tabac qui a été mis sur le marché avant le 1^{er} janvier 1990 par une entreprise juridiquement et financièrement distincte de toute entreprise qui fabrique, importe ou commercialise du tabac ou un produit du tabac. La création de tout lien juridique ou financier entre ces entreprises rend caduque cette dérogation. »

« Art. 9. - I. - Les teneurs maximales en goudron des cigarettes sont fixées par un arrêté du ministre chargé de la santé.

« II. - Chaque unité de conditionnement du tabac ou des produits du tabac doit porter selon des modalités précisées par arrêté du ministre chargé de la santé la mention : "Nuit gravement à la santé".

« III. - Chaque paquet de cigarettes porte mention :

« 1^o De la composition intégrale, sauf, s'il y a lieu, en ce qui concerne les filtres ;

« 2^o De la teneur moyenne en goudron et en nicotine.

« Un arrêté du ministre chargé de la santé fixe les modalités d'inscription de ces mentions obligatoires, les méthodes d'analyse permettant de mesurer la teneur en nicotine et en goudron et les méthodes de vérification de l'exactitude des mentions portées sur les paquets.

« Chaque paquet de cigarettes porte, en outre, dans les conditions fixées par un arrêté du ministre chargé de la santé, un message de caractère sanitaire.

« IV. - Les unités de conditionnement du tabac et des produits du tabac produites avant le 31 décembre 1991 qui ne seraient pas conformes aux dispositions des paragraphes II et III ci-dessus peuvent être commercialisées jusqu'au 31 décembre 1992 en ce qui concerne les cigarettes et jusqu'au 31 décembre 1993 en ce qui concerne les autres produits du tabac, à condition toutefois, d'une part, de comporter mention de la composition intégrale, sauf, s'il y a lieu, en ce qui concerne les filtres, et de la teneur moyenne en goudron et en nicotine et, d'autre part, d'indiquer, en caractères parfaitement apparents, la mention : "abus dangereux". »

« Art. 12. - Les infractions aux dispositions du présent titre sont punies d'une amende de 50 000 F à 500 000 F. En cas de propagande ou de publicité interdite le maximum de l'amende peut être porté à 50 p. 100 du montant des dépenses consacrées à l'opération illégale.

« En cas de récidive, le tribunal peut interdire pendant une durée de un à cinq ans la vente des produits qui ont fait l'objet de l'opération illégale.

« Le tribunal ordonne, s'il y a lieu, la suppression, l'enlèvement ou la confiscation de la publicité interdite aux frais des délinquants.

Décret no 92-478 du 29 mai 1992 fixant les conditions d'application de l'interdiction de fumer dans les lieux affectés à un usage collectif et modifiant le code de la santé publique (deuxième partie; Décrets en Conseil d'Etat)

NOR : SANP9201055D

Le Premier ministre, Sur le rapport du ministre de la santé et de l'action humanitaire, Vu le code de la santé publique; Vu le code de travail; Vu le code pénal, et notamment son article R.25; Vu la loi no 76-616 du 9 juillet 1976 relative à la lutte contre le tabagisme, modifiée par la loi no 91-32 du 10 janvier 1991, relative à la lutte contre le tabagisme et l'alcoolisme, et notamment son article 16; Vu le décret du 22 mars 1942 modifié sur la police, la sûreté et l'exploitation des voies ferrées d'intérêt général et d'intérêt local; Le Conseil d'Etat entendu,

Décète:

TITRE Ier DISPOSITIONS GENERALES

Art. 1er. - L'interdiction de fumer dans les lieux affectés à un usage collectif prévue par l'article 16 de la loi du 9 juillet 1976 susvisée s'applique dans tous les lieux fermés et couverts accueillant du public ou qui constituent les lieux de travail. Elle s'applique également dans les moyens de transport collectif et, en ce qui concerne les écoles, collèges et lycées publics et privés, dans les lieux non couverts fréquentés par les élèves pendant la durée de cette fréquentation.

Art. 2. - L'interdiction de fumer ne s'applique pas dans les emplacements qui, sauf impossibilité, sont mis à la disposition des fumeurs, au sein des lieux visés à l'article 1er du présent décret. Ces emplacements sont déterminés par la personne ou l'organisme, privé ou public, sous l'autorité duquel sont placés ces lieux, en tenant compte de leur volume, disposition, condition d'utilisation, d'aération et de ventilation et de la nécessité d'assurer la protection des non-fumeurs.

Art. 3. - Sans préjudice des dispositions particulières du titre II du présent décret, les emplacements mis à disposition des fumeurs sont soit des locaux spécifiques, soit des espaces délimités. Ces locaux ou espaces doivent respecter les normes suivantes: a) Débit minimal de ventilation de 7 litres par seconde et par occupant, pour les locaux dont la ventilation est assurée de façon mécanique ou naturelle par conduits; b) Volume minimal de 7 mètres cubes par occupant, pour les locaux dont la ventilation est assurée par des ouvrants extérieurs. Un arrêté pris par le ministre de la santé conjointement, s'il y a lieu, avec le ministre compétent, peut établir des normes plus élevées pour certains locaux en fonction de leurs conditions d'utilisation.

Art. 4. - I. - Sous réserve de l'application des articles suivants: dans les établissements mentionnés aux articles L.231-1 et L.231-1-1 du code du travail, il est interdit de fumer dans les locaux clos et couverts, affectés à l'ensemble des salariés, tels que les locaux d'accueil et de réception, les locaux affectés à la restauration collective, les salles de réunion et de formation, les salles et espaces de repos, les locaux réservés aux loisirs, à la culture et au sport, les locaux sanitaires et médico-sanitaires.

II. - L'employeur établit, après consultation du médecin du travail, du comité d'hygiène et de sécurité et des conditions de travail ou, à défaut, des délégués du personnel: a) Pour les locaux mentionnés au I ci-dessus, un plan d'aménagement des espaces qui peuvent être, le cas échéant, spécialement réservés aux fumeurs; b) Pour les locaux de travail autres que ceux prévus au I ci-dessus, un plan d'organisation ou d'aménagement destiné à assurer la protection des non-fumeurs. Ce plan est actualisé en tant que de besoin tous les deux ans.

Art. 5. - La décision de mettre des emplacements à la disposition des fumeurs est soumise à la consultation, lorsqu'elles existent, des instances représentatives du personnel compétentes en matière d'hygiène, de sécurité et de conditions de travail, ainsi que du médecin du travail. Cette consultation est renouvelée au moins tous les deux ans.

Art. 6. - Une signalisation apparente rappelle le principe de l'interdiction de fumer dans les lieux visés à l'article 1er du présent décret, et indique les emplacements mis à la disposition des fumeurs.

Art. 7. - Les dispositions du présent décret s'appliquent sans préjudice des dispositions législatives et réglementaires concernant l'hygiène et la sécurité, notamment celle du titre III du livre II du code du travail.

TITRE II DISPOSITIONS PARTICULIERES A CERTAINS LIEUX AFFECTES A UN USAGE COLLECTIF ET AUX MOYENS DE TRANSPORT COLLECTIF

Art. 8. - Dans l'enceinte des établissements d'enseignement publics et privés, ainsi que dans tous les locaux utilisés pour l'enseignement, des salles spécifiques, distinctes des salles réservées aux enseignants, peuvent être mises à la disposition des enseignants et des personnels fumeurs. En outre, dans l'enceinte des lycées, lorsque les locaux sont distincts de ceux des collèges, et dans les établissements publics et privés dans lesquels sont dispensés l'enseignement supérieur et la formation professionnelle, des salles, à l'exclusion des salles d'enseignement, de travail et de réunion, peuvent être mises à la disposition des usagers fumeurs.

Art. 9. - Dans les locaux à usage collectif utilisés pour l'accueil et l'hébergement des mineurs de moins de seize ans, ceux-ci n'ont pas accès aux emplacements mis à la disposition des fumeurs.

Art. 10. - Il est ajouté au décret du 22 mars 1942 susvisé un article 74-1 ainsi rédigé: <<Art. 74-1. - Dans les gares routières et ferroviaires, des salles ou zones d'attente peuvent être mises à la disposition des fumeurs. <<A l'exception des services de transports publics urbains et de la région Ile-de-France, dans les trains comportant des places assises, des emplacements peuvent être réservés aux fumeurs, dans la limite de 30 p. 100 de ces places. Dans les rames indéformables, les places réservées aux fumeurs sont situées dans des voitures distinctes. <<Dans les voitures des trains comportant des places couchées, l'interdiction de fumer ne s'applique pas à l'une des deux plates-formes de chaque voiture. <<Dans tous les cas, il doit être tenu compte de la nécessité d'assurer la protection des non-fumeurs.>>

Art. 11. - Dans les aéronefs commerciaux français ou exploités conformément à la réglementation française, à l'exception des vols intérieurs d'une durée inférieure à deux heures, des places peuvent être réservées aux fumeurs à condition que la disposition des places permette d'assurer la protection des non-fumeurs.

Art. 12. - A bord des navires de commerce et à bord des bateaux de transports fluviaux, y compris les bateaux stationnaires recevant du public, exploités conformément à la réglementation française, une organisation des espaces, éventuellement modulable, peut être prévue pour mettre des places à la disposition des fumeurs, dans la limite de 30 p. 100 de la surface des salles à usage de bar, de loisirs et de repos et de celle des cabines collectives.

Art. 13. - Dans les locaux commerciaux, où sont consommés sur place des denrées alimentaires et des boissons, à l'exception des voitures-bar des trains, une organisation des lieux, éventuellement modulable, peut être prévue pour mettre des espaces à la disposition des usagers fumeurs.

TITRE III SANCTIONS

Art. 14. - Sera puni de l'amende prévue pour les contraventions de la 3e classe quiconque aura fumé dans l'un des lieux visés à l'article 1er du présent décret, hors d'un emplacement mis à la disposition des fumeurs. Sera puni de l'amende prévue pour les contraventions de la 5e classe: a) Quiconque aura réservé aux fumeurs des emplacements non conformes aux dispositions du présent décret; b) Quiconque n'aura pas respecté les normes de ventilation prévues par l'article 3 du présent décret; c) Quiconque n'aura pas mis en place la signalisation prévue à l'article 6 du présent décret.

Art. 15. - Il est ajouté à l'article 80-2 du décret du 22 mars 1942 susvisé un alinéa ainsi rédigé: <<Sera puni de l'amende prévue pour les contraventions de la 3e classe quiconque aura fumé hors d'un emplacement mis à la disposition des fumeurs.>>

TITRE IV DISPOSITIONS FINALES

Art. 16. - I. - Le décret no 77-1042 du 12 septembre 1977 relatif aux interdictions de fumer dans certains lieux affectés à un usage collectif où cette pratique peut avoir des conséquences dangereuses pour la santé, ainsi que le 7^o du premier alinéa de l'article 74 du décret du 22 mars 1942 susvisé sont abrogés. II. - Au troisième alinéa de

l'article 1er du décret du 22 mars 1942 susvisé, les mots <<les articles 6, 73, 74>> sont remplacés par les mots <<les articles 6, 73, 74, 74-1...>>.

Art. 17. - A compter du 1er janvier 1993: I. - Il est inséré dans le code de la santé publique (deuxième partie: Décrets en Conseil d'Etat) un livre III intitulé: <<Lutte contre les fléaux sociaux>>. II. - Le titre VIII de ce livre est intitulé: <<Lutte contre le tabagisme>> et comprend un chapitre 1er intitulé: <<Interdiction de fumer dans les lieux affectés à un usage collectif>>. Ce chapitre comprend les articles R.355-28-1 à R.355-28-13. III. - Les articles 1er à 9 et 11 à 14 du présent décret deviennent respectivement les articles R.355-28-1 à R.355-28-13 du code de la santé publique. IV. - A l'article R.355-28-3, les mots: <<du titre II du présent décret>> sont remplacés par: <<des articles R.355-28-8 à R.355-28-12, et de l'article 74-1 du décret du 22 mars 1942 modifié sur la police, la sûreté et l'exploitation des voies ferrées d'intérêt général et d'intérêt local>>; à l'article R.355-28-13, les mots: <<aux dispositions du présent décret>> sont remplacés par: <<aux dispositions du présent chapitre et de l'article 74-1 du décret du 22 mars 1942 modifié sur la police, la sûreté et l'exploitation des voies ferrées d'intérêt général local>>.

Art. 18. - Le ministre d'Etat, ministre de l'éducation nationale et de la culture, le ministre d'Etat, ministre de la fonction publique et des réformes administratives, le garde des sceaux, ministre de la justice, le ministre de l'intérieur et de la sécurité publique, le ministre de la défense, le ministre de l'économie et des finances, le ministre du budget, le ministre de l'équipement, des transports et du logement, le ministre de l'industrie et du commerce extérieur, le ministre du travail, de l'emploi et de la formation professionnelle, le ministre de l'agriculture et de la forêt, le ministre des affaires sociales et de l'intégration, le ministre de la santé et de l'action humanitaire, le ministre des postes et télécommunications, le ministre de la jeunesse et des sports, le ministre délégué au commerce et à l'artisanat, le ministre délégué au tourisme, le secrétaire d'Etat à l'enseignement technique, le secrétaire d'Etat à la communication, le secrétaire d'Etat aux transports routiers et fluviaux et le secrétaire d'Etat à la mer sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au Journal officiel de la République française et qui entrera en vigueur à compter du premier jour du sixième mois suivant sa publication au Journal officiel.

Fait à Paris, le 29 mai 1992.

Document n° 3
page 1/10

LA SANTÉ EN CHIFFRES

TABAC



MINISTÈRE DE L'EMPLOI
ET DE LA SOLIDARITÉ
SECRETARIAT D'ÉTAT À LA SANTÉ
ET À L'ACTION SOCIALE



PRÉSENTATION

(3)

La lutte contre le tabagisme mobilise depuis plus de vingt ans beaucoup d'acteurs de santé publique. C'est au cours des années soixante-dix que les premières grandes initiatives ont été prises. Elles ont eu d'emblée différentes dimensions (législatives, éducatives...) et ont pris de multiples formes (communication publicitaire, actions de terrain...). Cependant, les résultats obtenus n'ont pas toujours été à la hauteur de l'espoir qui avait été mis dans ces programmes qui se sont révélés insuffisants face à la force des habitudes et à la détermination de certains lobbies qui défendent de puissants enjeux économiques.

Le début des années quatre-vingt-dix a marqué un tournant dans cette action de prévention. La loi du 10 janvier 1991, dite loi Evin, en a été la mesure majeure. Elle a interdit la publicité directe et indirecte, a favorisé une progression significative des prix, a limité les lieux où il était possible de fumer... Par ailleurs, l'ensemble de ces dispositions s'installait dans un pays où l'image du fumeur avait fortement évolué grâce aux campagnes qui se sont succédées année après année, et aux preuves qui se sont accumulées progressivement concernant l'effet délétère majeur de cette addiction sur la santé des populations. Les risques liés au tabagisme passif en illustrent parfaitement aujourd'hui toute la réalité et l'importance.

L'objectif de ce document est de présenter de façon synthétique des données actualisées et évolutives sur la mortalité, la morbidité, les opinions et les comportements vis-à-vis du tabac. Ces résultats proviennent, pour la majorité d'entre eux, d'enquêtes réalisées par le Comité français d'éducation pour la santé (CFES) dans le cadre des programmes nationaux de prévention de la Caisse nationale de l'assurance maladie des travailleurs salariés (Cnamts) et du CFES, et plus particulièrement des Baromètres Santé soutenus par différents partenaires dont le ministère de l'Emploi et de la Solidarité. Certains chiffres sont aussi issus de travaux récents de l'Institut national de la santé et de la recherche médicale (Inserm) et de l'Organisation mondiale de la santé (OMS), ainsi que de publications du Haut Comité de la santé publique (HCSP) et du Centre international de recherche sur le cancer (Circ).

SOMMAIRE

INTRODUCTION 5

MORTALITÉ ET MORBIDITÉ 6

Première cause de mortalité évitable en France : le tabac

Des différences selon le sexe

Des différences selon l'âge

Conséquences du tabagisme actif sur la morbidité et la mortalité

Femmes, femmes enceintes et tabac

Le tabagisme passif : des risques de mieux en mieux connus

CONSOMMATION DE TABAC 9

Les ventes

Les déclarations des adultes (18 ans et plus)

Les déclarations des jeunes (12-18 ans)

OPINIONS ET RAPPORT A LA LOI 15

CONCLUSION 16

RÉFÉRENCES BIBLIOGRAPHIQUES 17

ORGANISMES RESSOURCES 18

SITES INTERNET 18

INTRODUCTION

Les conséquences du tabagisme sur la santé ont été formellement démontrées dès les années cinquante et sont maintenant bien connues. Le nombre de décès dus au tabac est estimé aujourd'hui à 548 000 par an dans l'Union européenne et 60 000 en France, soit plus d'un décès sur neuf⁽¹⁾. Au vu des tendances passées et actuelles de consommation, des prévisions pour 2025 évaluent le nombre de morts liées au tabac, pour la France, à 160 000 dont 50 000 chez la femme, soit dix fois plus qu'aujourd'hui⁽¹⁾. Au regard de ces chiffres, la surveillance des données épidémiologiques en termes de mortalité, de morbidité et de consommation constitue une priorité.

Rappel de quelques définitions

Fumeur : personne qui fume, même de temps en temps.

Fumeur occasionnel : personne qui fume moins d'une cigarette par jour.

Fumeur régulier : personne qui fume au moins une cigarette par jour.

Ce texte a été rédigé par et sous la responsabilité éditoriale d'Annie Velter (Comité français d'éducation pour la santé) et François Baudier (Caisse nationale de l'assurance maladie des travailleurs salariés). Il s'appuie pour partie sur les travaux du groupe Indicateurs des données tabac composé de Gérard Badeyan (Direction de la recherche, des études, de l'évaluation et des statistiques), François Beck (Observatoire français des drogues et des toxicomanies), Michel Dépinoy et Christiane Dressen (Comité français d'éducation pour la santé), Danielle Fontaine (Fédération nationale des observatoires régionaux de la santé), Catherine Hill (Institut Gustave Roussy), Albert Hirsch (Hôpital Saint-Louis), Françoise Hodebar (Direction générale de la santé), Serge Karsenty (Centre national de la recherche scientifique), Annie Sasco (Centre international de recherche sur le cancer), Karen Slama (Union internationale contre la tuberculose et les maladies respiratoires) que nous tenons ici à remercier pour leur précieuse collaboration.

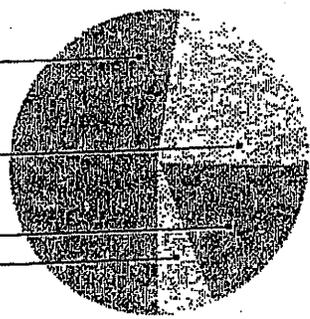
MORTALITÉ ET MORBIDITÉ

Première cause de mortalité évitable en France : le tabac

En 1995, en France, 60 000 morts sont directement ou indirectement imputables à l'usage du tabac, soit plus d'un décès sur neuf^[2]. La figure ① présente les principales causes de décès liés au tabac.

FIGURE 1
Répartition du nombre de décès suivant les principales maladies liées à l'usage du tabac en 1995

- 31 500 Cancers (poumon, oesophage, voies aérodigestives supérieures, vessie...)
- 14 000 Maladies cardio-vasculaires (maladies des artères coronaires, accidents vasculaires cérébraux...)
- 11 000 Maladies de l'appareil respiratoire (bronchite chronique, emphysème...)
- 3 500 Causes diverses

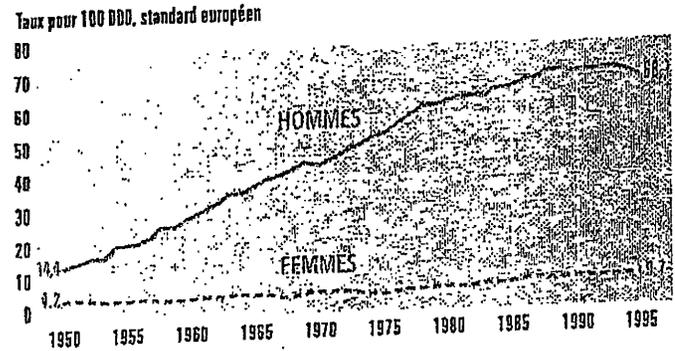


Des différences selon le sexe

Actuellement, le nombre de décès liés au tabac est beaucoup plus important dans la population masculine que féminine; 57 000 décès masculins sont attribuables au tabac—soit 21 % de l'ensemble de la mortalité masculine— et 3 000 décès féminins—soit 1 % de la mortalité féminine—. Pourtant, des évolutions sont perceptibles. Par exemple, pour le cancer du poumon, la mortalité est croissante chez la femme (et ce phénomène devrait s'amplifier dans les années à venir), alors que chez les hommes, on note une amorce de décroissance, mais avec des taux toujours très supérieurs à ceux des femmes (figure ②).

FIGURE 2
Évolution de la mortalité par cancer du poumon selon le sexe de 1950 à 1995

(Source : Institut Gustave Roussy)



Des différences selon l'âge

C'est dans la population des 45 à 64 ans que le poids des conséquences du tabac est le plus important : 29 % des décès masculins et 4 % des décès féminins sont attribuables au tabac^[2] (figure ③). Ce sont les jeunes fumeurs d'hier qui forment le gros des décès enregistrés aujourd'hui. Ceci est d'ailleurs à rapprocher des 160 000 morts prévus en 2025, compte-tenu des niveaux de consommation observés aujourd'hui, chez les jeunes de 18 ans.

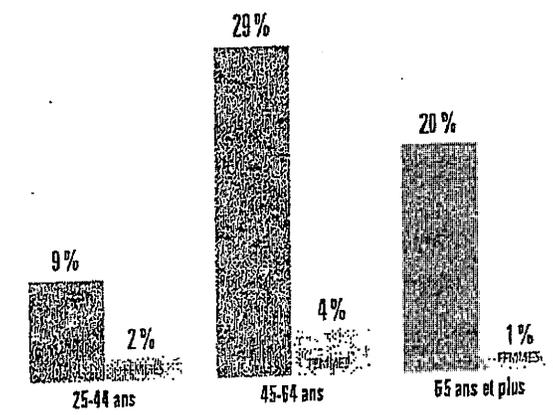
Conséquences du tabagisme actif sur la morbidité et la mortalité

Le fait de fumer accroît les risques de développer de nombreux cancers (poumon, voies aérodigestives supérieures, oesophage, vessie, pancréas, rein, col utérin...), des affections cardio-vasculaires (maladies des artères coronaires, artérites des membres inférieurs...), des maladies respiratoires chroniques...^[3]. Ainsi, en 1995, 20 323 décès masculins par cancer du poumon ont été enregistrés, dont 85 % sont attribuables au tabac^[2].

L'excès de risque encouru par un fumeur dépend de sa consommation moyenne journalière (dose de tabac), mais surtout de l'ancienneté de son tabagisme (durée). Le début du tabagisme avant l'âge de 15 ans multiplie par quatre le risque de cancer bronchique par rapport à un début après 25 ans. Si la durée totale du tabagisme en années est multipliée par 2, le risque de cancer est multiplié par 20^[4]. En conséquence, doubler la dose double l'excès de risque, doubler la durée multiplie l'excès de risque par vingt. Les effets bénéfiques de l'arrêt pour le fumeur sont donc très importants à court, moyen ou long terme^[2, 4].

FIGURE 3
Répartition du nombre de décès attribuables au tabagisme selon l'âge et le sexe en 1995

(Source : Institut Gustave Roussy)



Femmes, femmes enceintes et tabac

Certains risques sont spécifiques aux femmes : la consommation de tabac augmente les risques d'ostéoporose et du cancer du col utérin, et son association à la prise de contraceptifs oraux représente un danger pour le système cérébro-vasculaire. La consommation de tabac chez la femme risque de diminuer sa fertilité et d'augmenter le nombre de grossesses extra-utérines.

Par ailleurs, la consommation de tabac chez la femme enceinte (ou dans son entourage) comporte des risques spécifiques : un poids de naissance moyen plus faible du bébé, une probabilité augmentée de mort subite du nourrisson... [5, 6, 7].

Le tabagisme passif : des risques de mieux en mieux connus

L'exposition des jeunes enfants à la fumée de l'environnement (parents) augmente la fréquence des otites, des rhino-pharyngites et la gravité de l'asthme... [5, 6, 7].

Enfin, les risques de cancer du poumon sont significativement plus importants parmi les non-fumeurs qui vivent avec des proches fumeurs [8].

Deux types de données permettent d'étudier la consommation de tabac : les données de ventes et les résultats des sondages (aléatoires ou par quotas) sur des échantillons représentatifs de la population française.

Les ventes

Elles ont fortement augmenté à partir de 1950, pour atteindre un maximum de 6,8 grammes/adulte/jour en 1985. Depuis cette date, elles diminuent. Ainsi, les ventes de cigarettes ont reculé de 13 % pour la période 1992-1998 (figure 4).

Ce type de données permet d'étudier l'évolution globale de la consommation mais rencontre certaines limites : tous les pro-

duits vendus ne sont pas consommés ; ces chiffres ne tiennent pas compte de la contrebande ; une analyse des consommations par âge et sexe n'est pas possible.

Il faut donc se référer aussi à d'autres approches comme les sondages, qui permettent d'étudier la consommation de tabac — notamment par sexe et par âge —, mais également d'obtenir d'autres repères sociodémographiques et comportementaux concernant les fumeurs. Pourtant, les résultats émanant de ces études présentent également des biais : certains fumeurs se déclarent non fumeurs ou sous-déclarent leur consommation. L'importance de la pression sociale évolue au fil du temps et peut modifier le niveau de déclaration...

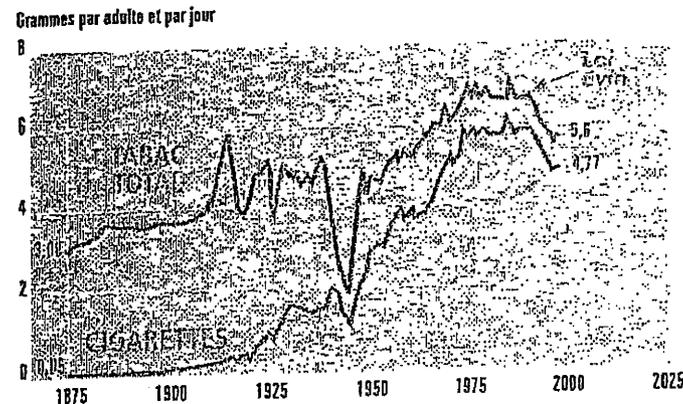


FIGURE 4
Évolution des ventes de tabac et de cigarettes par personne (15 ans et plus) et par jour en France

(Source : Institut Gustave Roussy, d'après des données provenant de la Seita et de l'Insee)

Les déclarations des adultes (18 ans et plus)

Évolution

Depuis plus de vingt ans, la prévalence du tabagisme a oscillé autour de 40 % (sujets déclarant fumer même de temps en temps). À partir de l'entrée en application

de la loi Evin, on observe une décroissance de la consommation déclarée d'environ 5 % (figure 5).

La figure 6 permet d'observer l'évolution du nombre moyen de cigarettes fumées par jour (chez les fumeurs réguliers). La moyenne est passée de 11,7 en 1977 à 13,7 en 1998.

FIGURE 5
Évolution de la proportion de fumeurs chez les adultes (18 ans et plus) selon le sexe
(Source : enquêtes du CFES)

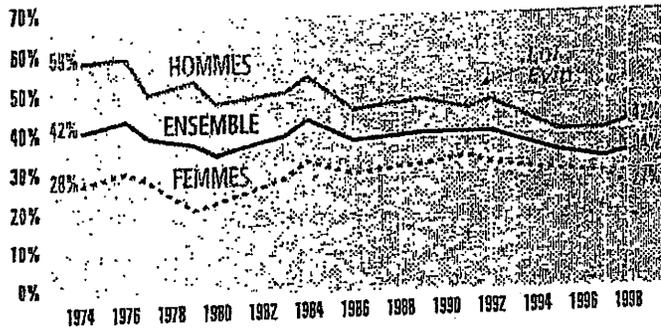
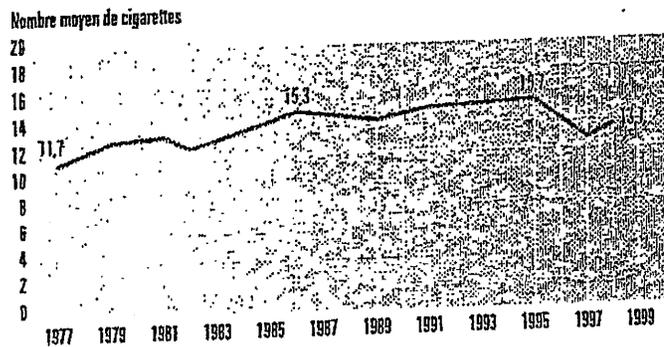


FIGURE 6
Évolution du nombre moyen de cigarettes consommées par les fumeurs (18 ans et plus)
(Source : enquêtes du CFES)



Comportement tabagique actuel

◆ Présentation

En 1998, lors de la dernière enquête menée par le CFES et la Cnamts auprès de la population française⁽¹⁾, un peu plus d'un tiers des adultes âgés de plus de 18 ans (35 %) déclarent fumer ne serait-ce que de temps en temps. Le pourcentage de fumeurs chez les hommes reste supérieur à celui des femmes (42 % contre 27 %). Le pourcentage de consommateurs de tabac diminue avec l'âge à partir de 35-49 ans aussi bien chez les hommes que chez les femmes (figure 7). Près de la moitié de la population âgée de 18 à 34 ans fume.

◆ Les quantités fumées

En 1998, les fumeurs réguliers consomment en moyenne 13,7 cigarettes par jour. Les hommes sont en moyenne de plus gros fumeurs (14,7 cigarettes par jour) que les femmes (12,4 cigarettes).

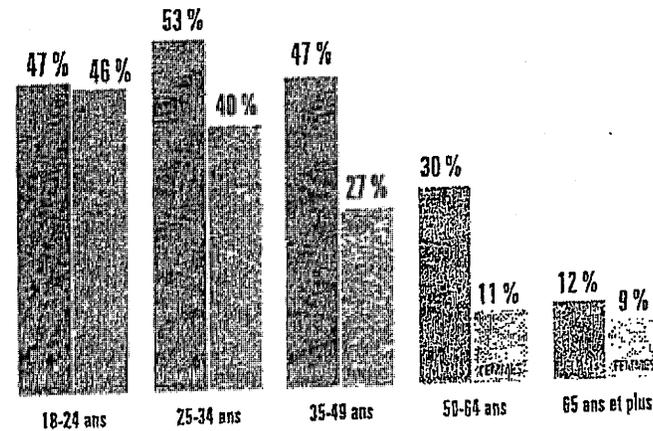


FIGURE 7
Pourcentage de consommateurs de tabac selon l'âge et le sexe (18 ans et plus)
(Source : enquête Ifop pour le CFES et la Cnamts - État des lieux du tabacage tabagique n. août 1998)

Les quantités consommées par les fumeurs progressent régulièrement avec l'âge, jusqu'à 49 ans pour les deux sexes confondus (figure 8)). Le niveau de consommation est également lié à l'ancienneté tabagique : les personnes qui fument depuis moins de dix ans consomment 10,6 cigarettes en moyenne par jour, contre 14,8 pour les fumeurs dont la consommation est égale ou supérieure à dix ans.

◆ Les changements de comportements

Au cours des douze derniers mois, plus de la moitié des fumeurs âgés de 18 ans et plus n'ont pas changé leur consumma-

tion (61 %), 17 % ont diminué et 10 % se sont mis à fumer des cigarettes légères.

31 % des fumeurs ont tenté d'arrêter au cours de l'année 1998. Les jeunes adultes (moins de 35 ans) sont plus nombreux à avoir essayé de modifier leur comportement (figure 9)).

Un peu plus d'un tiers des fumeurs âgés de 18 ans et plus (39 %) envisagent d'arrêter de fumer dans un avenir proche. Cette envie passe de 24 % pour les fumeurs âgés de 18 à 24 ans à un maximum de 31 % pour les 35-49 ans.

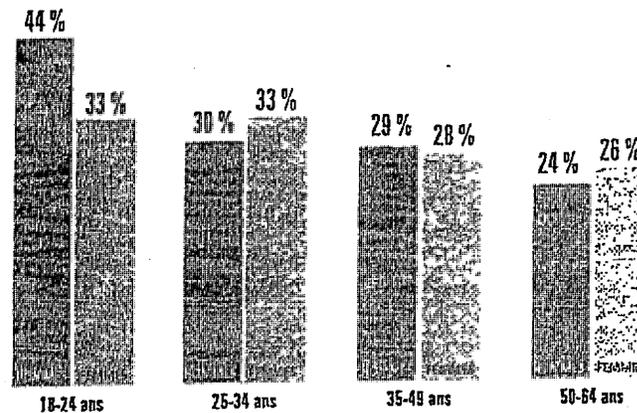


FIGURE 9
Pourcentage de fumeurs ayant tenté d'arrêter de fumer au cours de l'année écoulée selon l'âge et le sexe (18 ans et plus)

Les données concernant la tranche d'âge 65 ans et plus ne sont pas représentées ici du fait de la faiblesse de leur effectif (n < 15).

(Source : enquête Ifop pour le CFES « État des lieux du sevrage tabagique », août 1998)

Les déclarations des jeunes (12-18 ans)

Évolution

Depuis 1977, une décroissance du pourcentage d'adolescents français déclarant fumer (même de temps en temps) est observée. Ainsi, en 1977, la proportion de fumeurs de 12-18 ans atteignait 46 % ; en 1997, elle s'élève à 25 % ⁽¹⁰⁾. Ceci est vrai aussi bien chez les garçons que chez les filles, avec une diminution au fil du temps de la différence entre les deux sexes.

Comportement tabagique actuel

◆ Présentation

En 1997, 25 % des jeunes âgés de 12 à 18 ans déclarent fumer (même de temps en temps). Parmi ceux-ci, plus des trois quarts fument régulièrement, soit 20 % des jeunes. Les consommateurs occasionnels représentent 5 % des jeunes ⁽¹⁰⁾.

FIGURE 8
Quantités de tabac fumées régulièrement selon l'âge et le sexe (18 ans et plus)

Les données concernant la tranche d'âge 65 ans et plus ne sont pas représentées ici du fait de la faiblesse de leur effectif (n < 15).

(Source : enquête Ifop pour le CFES et la Cnamts « État des lieux du sevrage tabagique », août 1998)

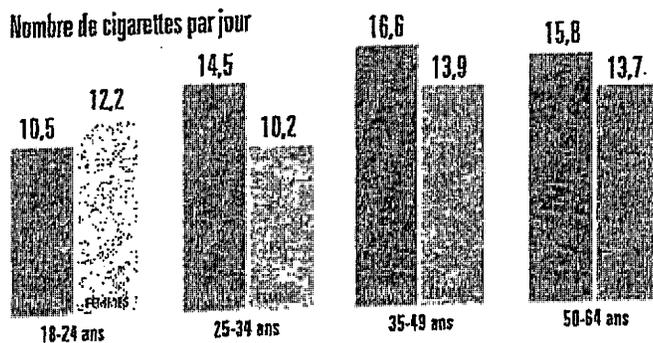
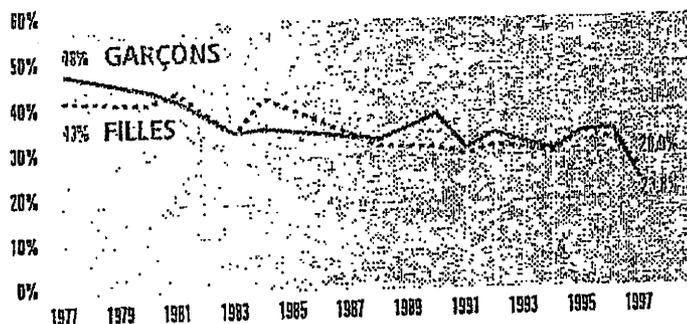


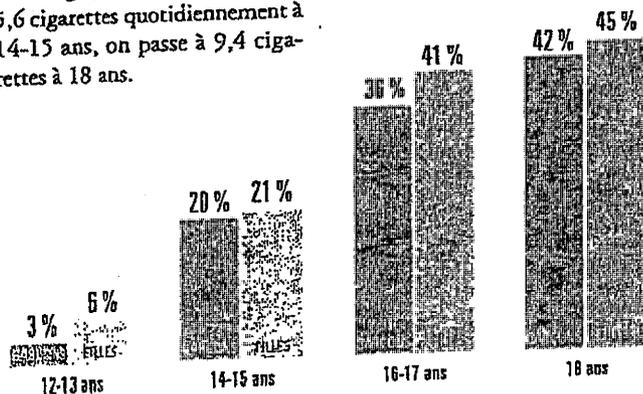
FIGURE 10
Évolution de la proportion de fumeurs chez les jeunes (12-18 ans) selon le sexe
(Source : Enquêtes CFES)



Le pourcentage de l'ensemble des jeunes fumeurs ne varie pas de façon significative entre les deux sexes (quel que soit l'âge), mais progresse beaucoup avec l'âge pour atteindre 43 % de fumeurs à 18 ans (figures 10 et 11).

◆ **Les quantités fumées**
Les fumeurs réguliers âgés de 12-18 ans consomment en moyenne 7,8 cigarettes par jour. Ces quantités augmentent avec l'âge : de 5,6 cigarettes quotidiennement à 14-15 ans, on passe à 9,4 cigarettes à 18 ans.

FIGURE 11
Pourcentage de consommateurs de tabac selon l'âge et le sexe (Jeunes de 12-18 ans)
(Source : Enquête santé Jeunes 97/98 - CFES)



◆ Les changements de comportements

Au cours des douze derniers mois, 50 % des jeunes fumeurs n'ont pas changé leur consommation, 10 % ont commencé à fumer et 19 % ont arrêté.

Parmi les jeunes fumeurs, 57 % souhaitent s'arrêter. Ce désir d'arrêt diminue sensiblement avec l'âge, mais reste toujours supérieur à 50 %.

Une très large majorité de personnes estime que les fumeurs sont dépendants du tabac comme d'une drogue (tableau 1). La même proportion considère que les consommateurs de tabac sont responsables des problèmes de santé qui leur arrivent. Plus de la moitié des personnes jugent justifié d'augmenter les taxes sur le tabac.

Une très large majorité de Français fumeurs (jeunes et adultes) disent respecter la loi. C'est dans les transports en commun qu'ils la transgressent le moins et dans les bars le plus (tableau 2). Pourtant, les deux tiers des adultes déclarent être gênés par la fumée des autres (10). Plus de la moitié des adolescents partagent cette gêne (10).

TABLEAU 1
Opinions sur le tabac : comparaisons entre le point de vue des jeunes et des adultes

	Jeunes (12-18 ans) favorables aux opinions suivantes	Adultes (18 ans et plus) favorables aux opinions suivantes
Les fumeurs sont dépendants du tabac comme d'une drogue	95%	95%
Les fumeurs sont responsables des problèmes de santé qui leur arrivent	95%	95%
Il est justifié d'augmenter les taxes sur le tabac	55%	55%

(Source : Baromètres santé Jeunes 97/98 et adultes 95/96 - CFES)

TABLEAU 2
Respect des zones non-fumeurs suivant le lieu, d'après les fumeurs

	Jeunes fumeurs 1997/1998	Adultes fumeurs 1995/1996
Lieu de travail	95%	95%
Transports en commun	95%	95%
Restaurant	95%	95%
Bar	95%	95%
Lieu couvert en général	95%	95%
École ou université	95%	95%

(Source : Baromètres santé Jeunes 97/98 et adultes 95/96 - CFES)

CONCLUSION

En 1999, le tabac reste un déterminant majeur de l'état de la santé de la population française. Ce produit est responsable d'un nombre important de décès prématurés. Une forte mobilisation reste donc toujours nécessaire.

Elle doit d'abord permettre de limiter l'initiation de ce processus addictif, qui survient souvent dès l'adolescence. C'est là tout l'enjeu de la prévention primaire, dont la mise en place est à envisager dans une approche globale et multifactorielle de la santé des enfants et des adolescents.

Par ailleurs, il est important de rendre plus accessibles les aides à l'arrêt pour les fumeurs qui souhaitent se libérer de cette habitude. C'est l'objectif prioritaire du programme que le CFES et la Cnamts ont engagé durant ces trois dernières années (1997-1999) : faciliter l'arrêt grâce au guide d'autosevrage, à la ligne « Tabac Info Service » (0 803 309 310), à la forte mobilisation des professionnels de santé (médecins, pharmaciens...). De même, le secrétariat d'Etat à la Santé et à l'Action sociale fait du sevrage tabagique une priorité de santé publique et souhaite favoriser l'accès aux traitements par une prise en charge thérapeutique renforcée et la vente libre de tous les substituts nicotiques en pharmacie.

Enfin, ces initiatives n'auraient qu'un effet limité si elles n'étaient pas développées dans un contexte législatif très précis. Le prix du tabac est augmenté régulièrement. Toute publicité directe et indirecte pour le tabac est interdite. Fumer dans les lieux à usage collectif est réglementé par un décret : la règle étant l'interdiction de fumer et le fait de pouvoir fumer une exception. Toutes ces dispositions complètent un plan de promotion de la santé dont chacune des facettes a son importance. C'est donc de la complémentarité des mesures législatives et éducatives, de leur mise en œuvre conjointe et d'une mobilisation sans défaillance, que des évolutions profondes seront possibles pour la santé des Français de demain. Dans cette perspective, la connaissance et le suivi d'indicateurs d'évolution de mortalité, de morbidité, d'opinions, d'attitudes et de comportements permettent d'évaluer l'impact des initiatives prises et d'envisager un éventuel réajustement des actions de promotion de la santé dans le domaine de la lutte contre le tabagisme.

RÉFÉRENCES BIBLIOGRAPHIQUES

- [1] HAUT COMITÉ DE LA SANTÉ PUBLIQUE. *La santé en France 1994-1998*. Paris : La Documentation française, 1998 : 167-77.
- [2] HILL C. Mortalité attribuable au tabagisme, bénéfice pour la santé de l'arrêt du tabac, et absence probable de bénéfice d'une réduction de la consommation. In : Anaes/Assistance publique. *L'arrêt de la consommation de tabac*. Conférence de consensus sur l'arrêt de la consommation du tabac. Paris, 8-9 octobre 1998. Paris : Éditions EDK, 1998 : 67-73.
- [3] MARTINET Y., BOHADANA A. Les affections liées à la consommation de tabac. In : *Le tabagisme. De la prévention au sevrage*. Paris : Masson, 1997 : 46-54.
- [4] VELTER A., GUILBERT P. *Données concernant la consommation du tabac, les risques qui lui sont imputables et les bénéfices attendus d'un arrêt de sa consommation*. Semaine des hôpitaux 1999 ; 75 : 369-83.
- [5] SASCO A.J. *Conséquences du tabagisme sur la mère et l'enfant*. Rev. Prat. 1993 ; 43 (10) : 1227-9.
- [6] KAMINSKI M. *Tabagisme « actif » et « passif » des femmes enceintes et risques pour l'enfant*. Bull. Acad. Nat. Méd. Paris : 1997 ; 181 : 30-9.
- [7] GUEGUEN C., LAGRUE G., JANSE-MAREC J. *Retentissement, sur le fœtus et l'enfant, du tabagisme pendant la grossesse*. J. Gynecol. Obstet. Biol. Reprod. 1995 ; 24 : 853-9.
- [8] MARTINET Y., BOHADANA A. Le tabagisme passif. In : MARTINET Y., BOHADANA A. *Le tabagisme. De la prévention au sevrage*. Paris : Masson, coll. abrégés, 1997 : 54-8.
- [9] IFOP. *État des lieux du sevrage tabagique. Résultats détaillés*. Vanves : CFES/Cnamts, 1998 : 56 p.
- [10] BAUDIER F., VELTER A. Tabac. In : Arènes J., Janvrin M.P., Baudier F. (sous la dir. de). *Baromètre santé jeunes 97/98*. Vanves : CFES, 1998 : 158-77.
- [11] GRIZEAU D., ARWIDSON P. Tabac : consommation et réglementation. In : Baudier F., Arènes J. (sous la dir. de). *Baromètre santé adultes 95/96*. Vanves : CFES, 1997 : 172-204.

ORGANISMES RESSOURCES

Caisse nationale de l'assurance maladie
des travailleurs salariés et son réseau
66, avenue du Maine - 75014 Paris

Comité français d'éducation pour la santé
et son réseau départemental et régional
2, rue Auguste Comte - BP 51 - 92174 Vanves cedex

Comité national contre les maladies respiratoires
et la tuberculose
66, boulevard Saint Michel - 75006 Paris

Fédération française de cardiologie
50, rue du Rocher - 75008 Paris

Ligue nationale contre le cancer
et ses comités départementaux
1, avenue Stephen Pichon - 75013 Paris

Ministère de l'Emploi et de la Solidarité -
Secrétariat d'État à la Santé et à l'Action sociale
8, avenue de Ségur - 75007 Paris

Mission interministérielle de lutte contre la drogue
et la toxicomanie
10, place des 5 martyrs du lycée Buffon - 75014 Paris

Office français du tabagisme
Service de santé publique - CH Pitié Salpêtrière -
75651 Paris cedex 12

SITES INTERNET

Site de l'OMS (*français, anglais*)
<http://www.who.int>

Site de l'association Action on Smoking & Health (*anglais*)
<http://www.ash.org.uk>

Site des médecins antitabac canadiens
(Physicians for a smoke free Canada) (*anglais*)
<http://www.smoke-free.ca>

Site du Centre national de documentation sur le tabac
et la santé (*français, anglais*)
<http://www.cctc.ca/ncth>

Site du secrétariat d'État à la Santé (*français*)
<http://www.sante.gouv.fr>

Site Tabac net (Paris sans tabac) (*français*)
<http://www-tabac-net.ap-hop-paris.fr>

Données d'octobre 1999

SERVICE MINUTEL ET TELEPHONE

3615 tabac-info (1,01€/min)



Le Parc des expositions de la Ville de Paris condamné pour non application de la loi Evin

Le Parc des expositions de la Ville de Paris condamné pour non application de la loi Evin

Paris, le 22 février 2005 - Dans un jugement du 20 janvier 2005 qui vient d'être publié, le Tribunal de Grande Instance de Nanterre a condamné les Sociétés d'exploitation du Parc des expositions de la Ville de Paris, Porte de Versailles, et Comexpo Paris, organisatrice du Salon du cheval 2002, à verser un euro symbolique de dommages et intérêts ainsi qu'une indemnité de 3.000 euros au Comité national contre le tabagisme (CNCT) pour non respect de la loi Evin du 10 janvier 1991 relative à l'interdiction de fumer dans les lieux affectés à un usage collectif.

Le Tribunal de grande instance de Nanterre, notant que « la lutte contre le tabagisme s'inscrit dans une politique sociale de protection de la santé publique et que l'attitude fautive des Sociétés d'exploitation du Parc des expositions de la Ville de Paris, Porte de Versailles, et Comexpo, occasionne un préjudice collectif, a notamment estimé que les organisateurs avaient manqué à leurs obligations légales d'information et de veiller au respect de l'interdiction de fumer à l'intérieur des locaux ». En effet, l'absence de l'affichage du règlement intérieur, de la signalisation apparente et systématique de l'interdiction de fumer, de même que la constance de nombreux visiteurs et exposants fumant à l'intérieur des halls, avaient pu être constatés par le CNCT et de nombreuses plaintes avaient été formulées auprès de l'association.

Dans une campagne télévisée de janvier 2005 (« La Parole aux victimes du tabagisme passif - La Liberté pour tous de respirer un air pur »), le CNCT avait rappelé que la fumée de tabac, étant à la fois toxique et cancérogène pour les fumeurs (fumeurs actifs) et les non-fumeurs (fumeurs passifs), l'interdiction totale de fumer à l'intérieur de locaux était le seul moyen d'y assurer à tous la liberté et le droit élémentaire de respirer un air pur.

De même, en septembre 2004, dans un appel solennel paru dans Le Figaro, le CNCT avait appelé à une simplification des textes en faveur d'une interdiction totale de fumer à l'intérieur des lieux publics, lieux de travail, dont bureaux, halls d'exposition, hôpitaux, restaurants, cafés, bars, discothèques, ...

A ce sujet, rappelons que la France a signé et ratifié la Convention-cadre pour le contrôle du tabac de l'Organisation mondiale de la santé, qui stipule notamment, dans son Article 8 : « La fumée du tabac entraîne la maladie, l'incapacité et la mort. (...) Il a été démontré que le seul moyen efficace de protéger les non-fumeurs contre l'exposition à la fumée ambiante dans un édifice donné est d'y instaurer une interdiction complète de fumer. »



Communiqué de presse

31 mars 2004

RESULTATS DEFINITIFS DE LA PREMIERE EVALUATION DE LA LOI EVIN EN MILIEU SCOLAIRE

L'Observatoire Français des Drogues et des Toxicomanies (OFDT) annonce la publication du rapport d'étude consacré à la première évaluation de la loi Evin dans les écoles, collèges et lycées, effectuée en 2002¹.

Menée à la demande de l'enseignement privé et public relevant du Ministère de l'Éducation Nationale et de la Mission Interministérielle de Lutte contre la Drogue et les Toxicomanies (MILDT), cette vaste enquête a permis, dix ans après l'entrée en vigueur de la loi Evin et de son décret d'application de mai 1992, de faire le point sur la mise en œuvre du volet tabac du texte dans les établissements scolaires. Ayant pour objectif affiché la protection des non-fumeurs, la loi a interdit de fumer dans les lieux publics et notamment les établissements scolaires sauf dans les emplacements explicitement réservés aux fumeurs ; le décret du 29 mai 1992 a, pour sa part, précisé les modalités de mise en place d'espaces fumeurs pour les mineurs de plus de 16 ans.

Au total, un échantillon représentatif de 600 responsables d'établissements, 1900 membres du personnel et 10 500 collégiens et lycéens avait été interrogé, dans le public comme dans le privé. Les premiers résultats, dévoilés dès 2002 (voir le communiqué de presse du 31 mai 2002) ont permis de cerner, pour les adultes comme pour les élèves, l'attitude vis-à-vis des règles en vigueur, les comportements et enfin les opinions.

Leur publication exhaustive, dans un contexte de renforcement de la lutte contre le tabac, est l'occasion de revenir sur les différentes réalités de l'application de la loi et d'identifier les problèmes concernant le personnel scolaire et les élèves en fonction des types d'établissement. Il apparaît ainsi que :

- Les établissements du premier degré, où seul le tabagisme des adultes est susceptible de poser problème, ne rencontrent pas de difficultés majeures et ce, même si la connaissance de la loi y est globalement moins précise que dans le secondaire. Dans ces établissements, le contexte du tabagisme est plutôt favorable et les taux de transgression des règles par les adultes très bas (moins de 10% des établissements).
- Dans le secondaire, s'agissant des personnels, le principe de la protection des non fumeurs, en particulier dans les salles des professeurs, apparaît mal appliqué dans deux tiers des cas. Globalement les personnels des collèges comme des lycées se déclarent majoritairement favorables à l'application de la loi mais les premiers semblent mieux respecter la règle que les seconds ; seuls un tiers des lycées ne connaissent pas de transgressions de la part des adultes contre six collèges sur dix.
- Concernant les élèves du secondaire, la mise en place de zones fumeurs dans certains collèges entre en contradiction avec l'interdiction d'accès aux moins de 16 ans. Le même problème se retrouve au lycée : 40% des établissements ont une zone fumeurs réservée aux élèves et l'accès des moins de 16 ans n'y est pas contrôlé. D'une façon générale, les lycéens concentrent sur eux la plus grande partie des difficultés d'application de la réglementation. Ils sont, compte tenu de leur âge, plus nombreux à fumer que les collégiens et sont un peu plus de la moitié à connaître la loi mais dans un quart des lycées seulement il n'y a jamais de transgression de la loi.

Cette situation conduit les auteurs du rapport à conclure leur état des lieux par un ensemble de recommandations. Il s'agit selon eux en priorité de :

¹KARSENTY (S), DIAZ-GOMEZ(C) - Le tabac en milieu scolaire. Résultats de la première évaluation de la loi Evin dans les écoles, collège et lycées (2002), OFDT, 2003, 164 p.

- Garantir, dans le primaire comme dans le secondaire, un meilleur respect de la réglementation concernant les salles des professeurs avec la suppression des autorisations d'y fumer.
- Mieux signaler les espaces autorisés aux fumeurs dans l'ensemble des établissements.
- Supprimer les zones fumeurs dans les collèges pour respecter l'interdiction d'accès aux élèves de moins de 16 ans. Respecter de même le principe de protection des moins de 16 ans dans les lycées.
- D'une manière plus générale dans le secondaire, améliorer la connaissance de la loi Evin auprès des chefs d'établissements (en rappelant par exemple que la création de zones fumeurs n'est nullement une obligation) afin de favoriser une application plus stricte des règles.

Ce rapport est disponible sur les sites www.ofdt.fr et www.drogues.gouv.fr

Contact presse :

Julie-Emilie Adès 01 41 62 77 46 julie-emilie.ades@ofdt.fr

Les ventes de cigarettes ont augmenté au premier semestre 2006, pour la première fois en quatre ans. La dissuasion par les prix, voulue par le gouvernement, semble avoir vécu.

Les ventes de tabac ont augmenté de 2,8 % en France sur les cinq premiers mois de l'année 2006, selon des chiffres publiés par la Confédération des débiteurs de tabac de France (CDTF). C'est la première fois, depuis 2002, qu'elles repartent à la hausse.

Le marché du tabac, en volume, a représenté près de 27 milliards d'unités vendues de janvier à mai, soit une progression de 2,8 % par rapport à la même période de 2005, selon le numéro d'été de la revue spécialisée de la confédération, *Le Losange*. Il s'agit d'une véritable inflexion de tendance : ces quatre dernières années, sous le coup d'une augmentation des taxes et de campagnes de prévention, les ventes avaient chuté de 34 %. Pour autant, elles restent inférieures de 25,8 % à celles de la même période de 2002.

DÉCEPTION DES ORGANISATIONS ANTI-TABAC

Cette reprise de la consommation en France s'explique par "*des raisons économiques, politiques et sociologiques*", souligne Robert Rochefort, directeur général du Centre de recherche pour l'étude et l'observation des conditions de vie (Credoc). Économiques : "*Les augmentations de prix ne sont efficaces que si elles sont continues, sinon elles s'émeussent*", relève Yves Martinet, président du Comité national contre le tabagisme (CNCT). Politiques : "*Le gouvernement hésite, contrairement à ce qu'il avait promis, à faire voter l'interdiction de fumer dans tous les lieux publics, y compris les bars. Cela entraînerait une nouvelle diminution de la consommation, comme en Italie ou en Irlande, où elle a baissé respectivement de 8 % et 6 %*", regrette M. Dautzenberg, président de l'Office français de prévention contre le tabagisme (OFPT). Sociologiques : "*Les jeunes reconnaissent le tabac comme dangereux mais pensent qu'il leur est possible de s'arrêter avant qu'il ne leur fasse du mal*", estime Robert Rochefort.

Pour leur part, les buralistes sont bien décidés à s'opposer aux "*ayatollahs de la lutte anti-tabac*", assène René Le Pape, président de la CDTF. "*Notre organisation professionnelle va travailler pour contrecarrer les mesures les plus radicales*", promet-il à ses adhérents dans l'éditorial du *Losange*.

Site IEP-Toulouse :

point européen : fin de la tolérance en Europe pour les fumeurs

Les temps sont durs pour les accros de la nicotine en France. Suivant le modèle irlandais, les cigarettes seront bientôt bannies des cafés, des boîtes de nuit et même des tabacs. Irlande, Italie, Suède, Espagne... La liste des pays européens qui luttent contre le tabagisme s'allonge de plus en plus.

L'Europe est-elle en passe de devenir une vaste zone non-fumeur ? Tour d'horizon des différentes initiatives nationales en matière de lutte contre le tabac.

Le décret antitabac en France

15 ans après son adoption, la loi Evin sera finalement appliquée. A compter du 1er février 2007, la cigarette devra se consumer hors des enceintes des lieux publics, entreprises, administrations, établissements scolaires, universités et magasins. Bars-tabac, restaurants, casinos, hôtels et discothèques bénéficieront toutefois d'un sursis jusqu'au 1er janvier 2008 pour installer des fumeurs clos et hermétiques, dotés d'extracteurs d'air, ou pour appliquer la tolérance zéro. L'annonce a été faite, dimanche 8 octobre, par le Premier ministre, Dominique de Villepin, lors de l'émission Le Grand Jury RTL-LCI- Le Figaro. Au vu des 60 000 morts par an directement imputables à la cigarette et des 5 000 dues au tabagisme passif, soit « en moyenne treize par jour », la mesure répondait à « un impératif de santé public qui s'impose à tous », a précisé le Premier ministre. Toute infraction sera punie d'une amende de 75 euros pour le fumeur et de 150 euros par fumeur pour le patron de l'établissement. Le décret prévoit également des aides au sevrage. L'Etat devrait ainsi débloquer 100 millions d'euros par an pour aider les fumeurs qui souhaiteraient arrêter. Toutes ces mesures du gouvernement français s'inscrivent dans un vaste mouvement européen, visant à lutter contre le tabagisme passif.

Les feux de l'amour s'allument à l'extérieur en Irlande et en Italie

Pas question aujourd'hui de franchir la porte d'un Pub sur l'île verte sans écraser d'abord sa cigarette. Le 24 mars 2004, l'Irlande a été le premier pays européen à imposer l'interdiction de fumer dans tous les lieux de travail (y compris les pubs et restaurants). Les amendes montent jusqu'à 3000 euros. Depuis le 10 janvier 2005, les Italiens eux-aussi boivent leur "expresso" sans fumer. La loi antitabac prévoit de lourdes sanctions pour les contrevenants : jusqu'à 275 euros d'amende pour le fumeur, le double si la cigarette a été allumée en présence d'une femme enceinte ou d'un enfant de moins de 12 ans ; de 220 à 2 200 euros pour les gérants d'établissements. Hiver comme été, les fumeurs noctambules se retrouvent désormais devant l'entrée des boîtes de nuit pour griller une cigarette. Plus agréable pour les Italiens choyés par le soleil que pour les Irlandais éprouvés par la pluie. Mais le nouveau lieu de rencontre a aussi provoqué l'émergence d'une nouvelle forme de socialisation : le « smirting » (smoking et flirting).

L'Allemagne – le contre-exemple

La publicité pour le tabac affichée partout, les rues bordées des distributeurs automatiques des cigarettes, les tables des bars couvertes des cendriers. Dans les stades pas question d'éteindre la cigarette. L'Allemagne – le paradis des fumeurs ? Au vu des dangers du tabagisme passif, l'interdiction de fumer dans les lieux publics est vivement discutée par les autorités politiques allemandes. Mais jusqu'ici, il n'existe pas d'interdiction générale. Depuis octobre 2002, le cabinet fédéral allemand a décrété l'interdiction de fumer dans les entreprises seulement. Cette réglementation ne concerne pas les restaurants, bars et autres lieux de travail qui sont ouverts au public. Les restaurants disposant d'une licence ont simplement le devoir de proposer des zones non-fumeurs. Il n'est pas interdit de fumer dans les transports ou les bâtiments gouvernementaux.

« Snus » : la solution suédoise pour arrêter de fumer

Le cancer du poumon et la crise cardiaque mettent fin à la vie de beaucoup de fumeurs. Les dangers du tabagisme sont connus. En France, six fumeurs sur dix expriment leur désir d'arrêter. Gomme et timbres sont proposés pour substituer à la nicotine. La dépendance est malheureusement souvent trop forte et les tentatives d'arrêter échouent. Le "Snus", pratique inventée en Suède, offre une possibilité de consommer la nicotine d'une manière différente. Le snus suédois, une poudre de tabac humide de différents arômes, est désormais proposée à la vente. Le tabac est, en effet, placé derrière la lèvre supérieure. Il ne faut ni mâcher ni avaler le snus. Lorsque le gouvernement suédois a imposé une réglementation stricte sur la consommation de cigarettes dans les lieux publics en juin 2005, les ventes de snus ont très fortement augmentées. Le snus n'affecte pas les poumons comme les cigarettes parce qu'il n'est pas inhalé. Les Suédois ont, en effet, le taux le plus bas de cancer du poumon en Europe. Le snus - une alternative inoffensive de consommation du tabac ? Les effets du snus ne sont pas encore suffisamment connus pour le dire. En dehors de la Suède qui bénéficie d'une dérogation, le snus n'est pas vendu en Union Européenne. Une directive de 2001 interdit aux Etats membres la mise sur le marché des tabacs oraux qui ne sont pas destinés à être fumés ou mâchés.

Le tabac et la loi

Le tabac est un produit licite. Sa production et sa vente sont réglementées.

PRODUCTION ET COMMERCE

Si depuis 1995 la production, l'importation et la distribution du tabac ne sont plus le monopole de la SEITA (Société d'exploitation industrielle des tabacs et allumettes), devenue ALTADIS (totalement privatisée et fruit de la fusion avec une société espagnole), la vente du tabac au détail reste un monopole d'État par l'intermédiaire des débitants de tabac.

LA RÉGLEMENTATION DE LA VENTE ET DE LA DISTRIBUTION

La loi prévoit :

- l'interdiction de vente de tabac aux mineurs de moins de 16 ans (loi du 31 juillet 2003) ;
- l'interdiction de la vente de paquets de moins de 20 cigarettes (loi du 26 juillet 2005) ;
- la fixation des teneurs maximales en goudron, en nicotine et en monoxyde de carbone des cigarettes ;
- l'obligation de faire figurer sur les paquets de cigarettes la teneur moyenne en goudron, en nicotine, et en monoxyde de carbone ainsi que l'un des deux avertissements généraux suivants : « Fumer tue » ou « Fumer nuit gravement à votre santé et à celle de votre entourage ». Un avertissement spécifique (extrait d'une liste de 14 avertissements établis par arrêté) est apposé sur l'autre côté du paquet, tel que « Fumer peut nuire aux spermatozoïdes et réduit la fertilité » ou « Fumer provoque un vieillissement de la peau »... Le numéro de téléphone de Tabac Info Service : 0825 309 310 est également inscrit sur les paquets. Ces mesures s'inscrivent dans l'application des directives européennes.

La loi interdit par ailleurs :

- toute propagande ou publicité, directe ou indirecte, en faveur du tabac ou des produits du tabac ;
- toute distribution gratuite ;
- toute opération de parrainage lorsqu'elle a pour objet la publicité en faveur du tabac.

LOI EVIN ET LIEUX COLLECTIFS La loi du 10 janvier 1991 sur la lutte contre le tabagisme, dite loi Evin, interdit de fumer dans les lieux affectés à un usage collectif, comme les entreprises, les bars et restaurants, les établissements scolaires, les transports collectifs. Toutefois, la loi prévoit la possibilité d'établir dans ces lieux des espaces réservés aux fumeurs, qui doivent :

- répondre à des normes de ventilation,
- être signalés de manière apparente.

En cas de non-respect de la loi,

- le fumeur s'expose à une amende pouvant s'élever jusqu'à 450 € (contravention de 3e classe),
- les propriétaires ou gérants d'établissements (bars, restaurants, entreprises, etc.) qui ont

fait le choix d'offrir un emplacement fumeurs à leurs clients et n'ont pas respecté les normes prévues par la loi risquent une amende pouvant s'élever jusqu'à 1 500 € (contravention de 5e classe).

Concernant les trains, les TGV sont devenus totalement non fumeurs depuis le 12 décembre 2004. Une mesure qui s'est étendue à l'ensemble des trains de la SNCF depuis la fin de l'année 2005. À la fin de l'année 2005, une réflexion a été entamée autour de la possibilité d'interdire le tabac dans tous les lieux publics.

LES CONVENTIONS INTERNATIONALES Dans le cadre de l'Organisation mondiale de la santé, une convention-cadre pour la lutte antitabac a été adoptée par la 56e Assemblée mondiale de la santé, signée le 16 juin 2003 par la France, puis ratifiée le 19 octobre 2004. Ce traité, premier accord international juridiquement contraignant sous l'égide de l'OMS, donne un cadre international à la lutte contre le tabac. Il prévoit des dispositions sur la publicité, les parrainages, les taxes, l'augmentation des prix, l'étiquetage, le commerce illicite et le tabagisme passif. Ce texte est entré en vigueur le 27 février 2005.

Tabac : de l'efficacité d'interdire

Article paru dans l'édition du 27.09.06

Le plaisir l'emportant sur la raison, la coercition associée à une sensibilisation au risque semble un très bon moyen d'inciter à arrêter de fumer

Ce n'est plus qu'une question de mois : le ministre de la santé l'a dit et répété, l'interdiction de fumer dans les lieux publics, à quelques exceptions près, sera totale dès le début de l'année 2007. « En aucun cas les aménagements envisagés pour certaines professions ne remettront en cause le principe général de l'interdiction », a précisé Xavier Bertrand, le ministre de la santé (Le Monde du 24 août). Il a mis en avant la reprise récemment constatée de la consommation de cigarettes : plus 2,8 % sur les cinq premiers mois de 2006, par rapport à la même période en 2005.

Si la mesure préconisée par le gouvernement est salubre sur le plan de la santé (600 000 décès prématurés sont imputés chaque année au tabac dans l'Union européenne, dont, en France, 66 000 par consommation et 5 000 par tabagisme passif), d'aucuns, fumeurs ou non, la considèrent comme une grave atteinte aux libertés individuelles.

Faut-il vraiment, pensent-ils, en passer comme aux Etats-Unis et dans le nord de l'Europe par cette mesure quasi totalitaire ? Placer un gendarme derrière chaque volute de fumée ? Ne vaudrait-il pas mieux promouvoir une éducation raisonnée contre les méfaits du tabac, et considérer le citoyen comme un sujet libre, conscient et responsable ? Utopie, répondent les experts. Si cela suffisait, tous les comportements de prise de risque devraient en effet céder devant les propositions philanthropiques et savantes des éducateurs - qu'il s'agisse de la prévention du sida ou des accidents de la route, des dangers liés aux drogues, aux abus d'alcool ou à une mauvaise alimentation. Or il n'en est rien.

Pourquoi ? Parce que le sujet « résiste », souligne Philippe Lecorps, professeur à l'Ecole nationale de la santé publique de Rennes, « pour des raisons qui lui sont propres, et auxquelles le plus souvent lui-même n'a pas accès ». Et sans, pour autant, être forcément irrationnel. « Aucune raison ne pourra jamais, à elle seule et à coup sûr, empêcher l'homme d'agir à sa guise, insiste ce psychologue (dans la revue La Santé de l'homme n° 377, mai-juin 2005). Il faut bien entendre cette petite musique du sujet, mi-être de raison, mi-être de l'inconscient. Acceptons-le, sa conduite, jugée défavorable par les acteurs de santé, ne relève pas de l'irrationalité - même si elle en donne l'apparence - mais témoigne de la force du désir à l'oeuvre dans l'agir humain. Et le désir, c'est l'envers de la raison. » Surtout quand sa réalisation est garante de plaisir.

Plaisir de fumer et de boire, plaisir de la vitesse ou de la sexualité sans entrave... Face à cette force d'attraction, la connaissance du danger ne suffit parfois pas pour résister. D'autant que la diffusion de ce savoir se fait elle-même de façon inégale, privilégiant les classes socioculturelles les plus élevées. Pour qu'elle concerne la majeure partie de la population, qu'elle soit propagée dans les établissements scolaires et médicaux, l'intervention d'une puissance régaliennne est donc nécessaire. Comme l'est, souvent, la réglementation pour que soient respectés les principes de précaution prônés par les experts.

« Chez l'adulte comme chez l'enfant, l'interdit peut être nécessaire et utile , mais à une condition : que ce ne soit pas la seule stratégie employée », affirme ainsi Philippe-Jean Parquet, professeur de psychiatrie de l'enfant et de l'adolescent à l'université du droit et de la santé de Lille, .

Auteur en 1997 d'un rapport ministériel sur la prévention contre la consommation des substances psychoactives, le Pr Parquet rappelle que, pour aider un « accro » à se libérer de sa dépendance, il faut aussi lui donner le désir de vivre en bonne santé, de se débrouiller seul pour modifier ses conduites, de demander de l'aide si besoin... Toutes stratégies globales d'éducation pour la santé qui, estime-t-il, « ont été mises, dans le cas de la prévention contre le tabagisme, en deuxième position par rapport à la stratégie coercitive ».

On est ainsi passé de la mise en garde (« Il n'est pas bon pour vous de fumer ») à l'injonction (« Vous ne devez pas fumer »), assortie d'une stigmatisation du fumeur. En oubliant que le tabac, longtemps accepté - voire valorisé - socialement avant d'être diabolisé, est une drogue dure, au sens d'une dépendance. Une drogue dont on ne peut se défaire d'un simple coup de volonté ni sans difficultés psychologiques et physiologiques.

Avec l'interdiction totale de fumer dans les lieux publics, l'Etat franchit aujourd'hui une étape supplémentaire : à l'argument sanitaire individuel, il ajoute un argument sécuritaire contre les dommages subis par la collectivité. Et un troisième, d'ordre moral : nous nous devons de respecter nos concitoyens et de participer collectivement à la lutte contre le tabagisme passif.

« Si ces trois maillons de la réflexion sont pris en compte dans l'énonciation d'une politique, l'ensemble constitue une méthode de prévention extrêmement positive, souligne le Pr Parquet. Par contre, si l'interdiction domine sur l'éducation, on aboutit à une infantilisation non respectueuse d'autrui. » Ce serait d'autant plus dommage que l'opinion publique semble prête à entendre raison : selon un sondage Ifop réalisé pour le compte du gouvernement et publié en mars, 78 % des Français seraient favorables à la mesure promise par le ministre de la santé.

mercredi 25 octobre 2006

La France sans tabac fait débat...

Pour les patrons de bars la nouvelle loi anti-tabac ne fait pas un carton. Ils sont nombreux à avoir peur de perdre des clients et voir leur chiffre d'affaire partir en fumée. Interview de XXXX, patron d'un bar en périphérie toulousaine.

Êtes-vous favorable à la nouvelle loi anti-tabac ?

Mon avis est assez partagé. Il est vrai que si je vous parle en temps qu'homme, je vous dirais bien entendu que d'un point de vue de santé publique, je suis favorable à cette loi. On ne peut que se réjouir d'une loi qui protégerait les victimes du tabagisme passif. Je vois tous les jours des personnes qui subissent les cigarettes de leur voisin de table, sans oser le dire.

Certains de vos collègues craignent une forte baisse de la fréquentation de leur bar, et donc de leur chiffre d'affaire. Qu'en est-il pour vous ?

Je dois être franc, et là, c'est le patron de bar qui vous parle, je pense aussi que cette loi risque bien de faire diminuer la fréquentation de mon bar. Je connais bon nombre de mes clients qui, s'ils ne peuvent pas accompagner leur café ou leur bière d'une cigarette ne viendront plus autant dans mon bar. Ils préféreront sans doute, boire leur café chez eux, où ils pourront allumer leur clope sans risquer une amende. Fumer quand on va dans un café, c'est une habitude pour de très nombreuses personnes. Je crois même que j'ai plus de clients fumeurs que non-fumeurs. Je me vois mal devoir virer certains de mes clients parce qu'ils refuseront de ne pas fumer...alors qu'il y en a, ça fait plus de 15 ans qu'ils viennent dans mon bar, pour prendre leur apéro, jouer aux cartes avec les copains et fumer leur cigarette !

La nouvelle loi prévoit un sursis jusqu'en janvier 2008 pour les bars-tabac, restaurants, hôtels, casinos et discothèques. Un sursis qui devrait leur permettre d'adapter progressivement leur locaux aux nouvelles normes, notamment par l'installation de fumoirs clos et d'extracteurs d'air. Quelles solutions envisagez-vous ?

Mon problème, c'est que mon bar n'a pas de terrasse. Je ne pourrais donc pas aménager un coin fumeur à l'extérieur, avec des lampes chauffantes par exemple, pour permettre à ma clientèle de s'installer dehors en hiver. C'est une solution qui est assez utilisée en Italie je crois. J'ai vu la même chose dans pas mal de bars à Paris aussi. Après, concernant l'installation de fumoirs clos avec extracteurs d'air, ce sont des aménagements qui demandent beaucoup d'argent, ça ne peut pas se faire du jour au lendemain. Je suis déjà entrain de réfléchir à tous ça. Si je ne suis pas en mesure d'aménager mon bar de cette manière, il ne me restera plus qu'à appliquer la "tolérance zéro" -comme ils disent- avec mes clients...Et là, c'est sûr que j'en perdrais quelques uns !

3 PERSONNES REPONDENT A LA QUESTION : "Êtes-vous favorable à la loi anti-tabac?"

Myriam, 21 ans, étudiante en droit

Complètement. Je suis non-fumeuse et lorsque je vais dans un bar pour boire mon café, je suis sans arrêt indisposée par les odeurs de cigarettes autour de moi. Et encore, ce n'est pas le pire. Lorsque je rentre chez moi après une soirée en boîte, je sens tellement la cigarette que j'ai l'impression d'avoir moi-même fumé deux paquets ! Je trouve ça anormal. J'aimerais pouvoir passer de bonnes soirées sans ingurgiter la fumer de tous ces "acros" autour de moi !

Gilles, 42 ans, commercial

Je suis moi-même fumeur, mais je suis quand même favorable à la loi. Je ne vois pas ce qui m'empêche d'aller dehors lorsque j'ai envie de me griller une petite cigarette. J'ai des enfants, je ne fume jamais devant eux pour ne pas les "intoxiquer". Et je serais content qu'ils ne

Sébastien, 30 ans, vendeur

Je ne suis pas favorable à cette loi. Je pense qu'elle est excessive. Il faut arrêter de considérer les tumeurs comme des "paras" de la société. Je suis fumeur, j'aimerais pouvoir continuer à fumer dans un bar lorsque je bois mon café. Je comprend bien entendu les non-fumeurs, je comprends que la fumée des autres peut être gênante. Mais ce n'est pas une raison pour exclure les fumeurs de la sorte. Après tout dans la plupart des bars, il existe déjà des coins "tumeurs" et "non-tumeurs". Alors pourquoi interdire totalement de fumer dans tous les lieux publics ?

Marie-Cécile ALBIGNAT

Décrets, arrêtés, circulaires

Textes généraux

Ministère de la santé et des solidarités

Décret n° 2006-1386 du 15 novembre 2006 fixant les conditions d'application de l'interdiction de fumer dans les lieux affectés à un usage collectif

NOR: SANX0609703D

Le Premier ministre,

Sur le rapport du ministre de la santé et des solidarités,

Vu le code pénal ;

Vu le code de procédure pénale ;

Vu le code de la santé publique, notamment son article L. 3511-7 ;

Vu le code du travail ;

Vu le décret du 22 mars 1942 modifié sur la police, la sûreté et l'exploitation des voies ferrées d'intérêt général et d'intérêt local ;

Le Conseil d'Etat entendu,

Décète :

Article 1

La section 1 du chapitre Ier du titre unique du livre V de la troisième partie du code de la santé publique est remplacée par les dispositions suivantes :

« Section 1

« Interdiction de fumer

dans les lieux affectés à un usage collectif

« Art. R. 3511-1. - L'interdiction de fumer dans les lieux affectés à un usage collectif mentionnée à l'article L. 3511-7 s'applique :

« 1° Dans tous les lieux fermés et couverts qui accueillent du public ou qui constituent des lieux de travail ;

« 2° Dans les moyens de transport collectif ;

« 3° Dans les espaces non couverts des écoles, collèges et lycées publics et privés, ainsi que des établissements destinés à l'accueil, à la formation ou à l'hébergement des mineurs.

« Art. R. 3511-2. - L'interdiction de fumer ne s'applique pas dans les emplacements mis à la disposition des fumeurs au sein des lieux mentionnés à l'article R. 3511-1 et créés, le cas échéant, par la personne ou l'organisme responsable des lieux.

« Ces emplacements ne peuvent être aménagés au sein des établissements d'enseignement publics et privés, des centres de formation des apprentis, des établissements destinés à ou régulièrement utilisés pour l'accueil, la formation, l'hébergement ou la pratique sportive des mineurs et des établissements de santé.

« Art. R. 3511-3. - Les emplacements réservés mentionnés à l'article R. 3511-2 sont des salles closes, affectées à la consommation de tabac et dans lesquelles aucune prestation de service n'est délivrée. Aucune tâche d'entretien et de maintenance ne peut y être exécutée sans que l'air ait été renouvelé, en l'absence de tout occupant, pendant au moins une heure.

« Ils respectent les normes suivantes :

« 1° Etre équipés d'un dispositif d'extraction d'air par ventilation mécanique permettant un renouvellement d'air minimal de dix fois le volume de l'emplacement par heure. Ce dispositif est entièrement indépendant du système de ventilation ou de climatisation d'air du bâtiment. Le local est maintenu en dépression continue d'au moins cinq pascals par rapport aux pièces communicantes ;

« 2° Etre dotés de fermetures automatiques sans possibilité d'ouverture non intentionnelle ;

« 3° Ne pas constituer un lieu de passage ;

« 4° Présenter une superficie au plus égale à 20 % de la superficie totale de l'établissement au sein duquel les emplacements sont aménagés sans que la superficie d'un emplacement puisse dépasser 35 mètre carrés.

« Art. R. 3511-4. - L'installateur ou la personne assurant la maintenance du dispositif de ventilation mécanique atteste que celui-ci permet de respecter les exigences mentionnées au 1° de l'article R. 3511-3. Le responsable de l'établissement est tenu de produire cette attestation à l'occasion de tout contrôle et de faire procéder à l'entretien régulier du dispositif.

« Art. R. 3511-5. - Dans les établissements dont les salariés relèvent du code du travail, le projet de mettre un emplacement à la disposition des fumeurs et ses modalités de mise en oeuvre sont soumises à la consultation du comité d'hygiène et de sécurité et des conditions de travail ou, à défaut, des délégués du personnel et du médecin du travail.

« Dans les administrations et établissements publics dont les personnels relèvent des titres Ier à IV du statut général de la fonction publique, le projet de mettre un emplacement à la disposition des fumeurs et ses modalités de mise en oeuvre sont soumises à la consultation du comité d'hygiène et de sécurité ou, à défaut, du comité technique paritaire.

« Dans le cas où un tel emplacement a été créé, ces consultations sont renouvelées tous les deux ans.

« Art. R. 3511-6. - Dans les lieux mentionnés à l'article R. 3511-1, une signalisation apparente rappelle le principe de l'interdiction de fumer. Un modèle de signalisation accompagné d'un message sanitaire de prévention est déterminé par arrêté du ministre chargé de la santé.

« Le même arrêté fixe le modèle de l'avertissement sanitaire à apposer à l'entrée des espaces mentionnés à l'article R. 3511-2.

« Art. R. 3511-7. - Les dispositions de la présente section s'appliquent sans préjudice des dispositions législatives et réglementaires relatives à l'hygiène et à la sécurité, notamment celles du titre III du livre II du code du travail.

« Art. R. 3511-8. - Les mineurs de moins de seize ans ne peuvent accéder aux emplacements mentionnés au premier alinéa de l'article R. 3511-2. »

Article 2

A la section unique du chapitre II du titre unique du livre V de la troisième partie du code de la santé publique, les articles R. 3512-1 et R. 3512-2 sont remplacés par les dispositions suivantes :

« Art. R. 3512-1. - Le fait de fumer dans un lieu à usage collectif mentionné à l'article R. 3511-1 hors de l'emplacement mentionné à l'article R. 3511-2 est puni de l'amende prévue pour les contraventions de la troisième classe.

« Art. R. 3512-2. - Est puni de l'amende prévue pour les contraventions de la quatrième classe le fait, pour le responsable des lieux où s'applique l'interdiction prévue à l'article R. 3511-1, de :

« 1° Ne pas mettre en place la signalisation prévue à l'article R. 3511-6 ;

« 2° Mettre à la disposition de fumeurs un emplacement non conforme aux dispositions des articles R. 3511-2 et R. 3511-3 ;

« 3° Favoriser, sciemment, par quelque moyen que ce soit, la violation de cette interdiction. »

Article 3

L'article 74-1 du décret du 22 mars 1942 susvisé est abrogé.

Article 4

L'article R. 48-1 du code de la procédure pénale est complété par un alinéa ainsi rédigé :

« 6° Contraventions réprimées par le code de la santé publique prévues par les articles R. 3512-1 et le 1° et 2° de l'article R. 3512-2. »

Article 5

Les dispositions du présent décret entrent en vigueur le 1er février 2007. Toutefois les dispositions des articles R. 3511-1 à R. 3511-8 et de l'article R. 3511-13 du code de la santé publique en vigueur à la date de publication du présent décret restent applicables jusqu'au 1er janvier 2008 aux débits permanents de boissons à consommer sur place, casinos, cercles de jeu, débits de tabac, discothèques, hôtels et restaurants.

Article 6

I. - Les dispositions du présent décret sont applicables à Mayotte à l'exception de l'article 3.

II. - Le chapitre unique du titre unique du livre VIII de la troisième partie du code de la santé publique est ainsi modifié :

1° L'article R. 3811-1 est ainsi rédigé :

« Art. R. 3811-1. - Les dispositions des articles R. 3221-2 à R. 3221-4, R. 3221-9 à R. 3221-11, R. 3511-1 à R. 3511-8, R. 3512-1 et R. 3512-2 sont applicables à Mayotte sous réserve des adaptations prévues par le présent chapitre. »

2° Il est créé après l'article R. 3811-3 un article R. 3811-4 ainsi rédigé :

« Art. R. 3811-4. - Pour l'application à Mayotte des articles R. 3511-5 et R. 3511-7, les renvois au code du travail doivent s'entendre comme intéressant le code du travail de Mayotte. »

Article 7

Le ministre de l'emploi, de la cohésion sociale et du logement, le ministre de l'éducation nationale, de l'enseignement supérieur et de la recherche, le garde des sceaux, ministre de la justice, le ministre de la santé et des solidarités, le ministre de la fonction publique, le ministre de l'outre-mer, le ministre de la jeunesse, des sports et de la vie associative, le ministre délégué à l'emploi, au travail et à l'insertion professionnelle des jeunes et le ministre délégué à l'enseignement supérieur et à la recherche sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au Journal officiel de la République française.

Fait à Paris, le 15 novembre 2006.

Dominique de Villepin

Par le Premier ministre :

Le ministre de la santé et des solidarités,
Xavier Bertrand
Le ministre de l'emploi,
de la cohésion sociale et du logement,
Jean-Louis Borloo

Le ministre de l'éducation nationale,
de l'enseignement supérieur
et de la recherche,
Gilles de Robien
Le garde des sceaux, ministre de la justice,
Pascal Clément
Le ministre de la fonction publique,
Christian Jacob
Le ministre de l'outre-mer,
François Baroin
Le ministre de la jeunesse, des sports
et de la vie associative,
Jean-François Lamour
Le ministre délégué à l'emploi, au travail
et à l'insertion professionnelle des jeunes,
Gérard Larcher
Le ministre délégué
à l'enseignement supérieur
et à la recherche,
François Goulard

Tribune
**Contre l'interdiction de fumer dans
les lieux publics**

Tribune du Collectif des Amoureux de l'Art de Vivre contre
l'interdiction de fumer dans les lieux publics

La Mission parlementaire d'information sur
l'interdiction du tabac dans les lieux publics va rendre
public les conclusions de ses travaux, sans avoir
accepté d'entendre les représentants des 16 millions
de fumeurs en France.

Cette absence de débat démocratique, au niveau
d'une mission parlementaire d'information, est une
première. Elle n'a pas non plus voulu tenir compte de
l'opinion des Françaises et des Français (sondage
IFOP du 15 septembre) qui dans leur immense
majorité, 86%, sont pour une coexistence séparée
entre fumeurs et non-fumeurs. Rien d'étonnant
toutefois, lorsque l'on examine la composition de ce
groupe, essentiellement constitué de personnalités
antitabac, pour qui dès le premier jour, « la messe
était dite ».

Le Collectif des Amoureux de l'Art de Vivre, qui
regroupe des centaines d'associations, clubs et
confréries, et plus de 60 000 signatures à ce jour,
milite pour une société tolérante, respectueuse des
droits des uns et des autres, et fraternelle.

La Mission parlementaire n'avait d'information que le
nom. Elle s'est comportée, comme un tribunal
d'exception, sans aucun respect pour les droits de la
défense.

Les Français répondront à cette dérive
prohibitionniste sur le terrain.

Document de synthèse

Le premier chapitre de ce rapport est consacré aux effets nuisibles du tabagisme sur la santé des individus et de l'ensemble de la population en Europe. Malgré les progrès réalisés en matière de lutte contre le tabac, le tabagisme reste la principale cause de mortalité et de morbidité dans l'Union européenne (UE). Chaque année, le tabagisme tue plus de 650.000 Européens et est responsable de plus d'un décès sur sept dans l'UE. Ajoutons à cela que plus de 13 millions de fumeurs/ex-fumeurs sont atteints d'une grave maladie chronique. L'on peut aujourd'hui affirmer avec certitude que la fumée du tabac constitue un risque majeur du point de vue de la santé environnementale, puisque le décès de dizaines de milliers d'Européens, non-fumeurs, lui est imputable. Enfin, pour plusieurs millions de personnes, le tabagisme passif constitue un facteur aggravant de pathologies sous-jacentes.

Le tabac endommage pratiquement chaque organe du corps humain et provoque ainsi de nombreuses maladies. Pourtant, l'étendue réelle des lésions et des troubles dus au tabagisme est encore méconnue. Aujourd'hui en effet, plus de 50 ans après la mise en évidence des premiers liens entre le tabac et le cancer bronchique, la liste des maladies provoquées par le tabagisme ne cesse de s'allonger. L'on peut toutefois affirmer que la moitié environ des fumeurs réguliers (qui ne deviendront jamais abstinents) mourront à cause du tabac et que ceux qui meurent prématurément à cause du tabac perdent en moyenne 22 années d'espérance de vie, dont une grande partie sera gâchée par une mauvaise santé.

Même si les divers pays d'Europe sont confrontés à différents stades de l'épidémie de tabagisme, il ne fait aucun doute qu'au cours des prochaines décennies, le tabac provoquera de nouveaux millions de décès et de pathologies parmi les fumeurs en Europe. Au sein de la population féminine, les décès imputables au tabac continuent d'augmenter, et l'ampleur réelle de l'épidémie chez les femmes est encore largement méconnue. Chez les hommes aussi, les taux de mortalité par cancer bronchique sont encore en hausse dans quatre Etats membres. Par ailleurs, le tabagisme est de plus en plus lié à la pauvreté et joue un grand rôle dans l'aggravation des inégalités de santé au sein de l'UE. Pour illustrer l'impact de la consommation de tabac dans l'UE, le rapport décrit dans les grandes lignes les tendances de mortalité dans cinq pays européens.

Vu le caractère parfaitement évitable de ces décès et pathologies, le chapitre 1 examine également le rôle important de la nicotine dans la dépendance tabagique et les effets particulièrement bénéfiques sur la santé de l'arrêt du tabac.

Le chapitre 2 montre à quel point tous les Etats membres de l'UE sont également concernés par la production, la fabrication, la distribution et la vente de produits du tabac. Avec seulement 1,3% d'exploitations européennes productrices de tabac, sur 0,1% des terres agricoles, la culture du tabac ne représente qu'une petite partie de l'activité agricole au sein de l'UE. En outre, la part de l'Europe dans la culture mondiale du tabac est en baisse depuis le milieu des années 1980.

Le tabac est néanmoins la culture la plus subventionnée par hectare en Europe. L'UE subventionne cette culture à hauteur de près de 1.000 millions € : 2,3% du budget de la Politique agricole commune et 1,1% du budget total de la Commission. L'UE a eu la sagesse de supprimer ces subventions d'ici à 2010.

(...)

Pour l'UE, le tabagisme représente une charge économique substantielle. Au bas mot, ces coûts s'élèveraient à 98–130 milliards €, soit 1,04–1,39% du produit domestique brut de la région pour 2000. Les coûts réels sont sans aucun doute plus élevés, et continueront à grimper en l'absence de mesures appropriées. Cet accroissement des coûts résultera des taux de tabagisme élevés dans les 10 nouveaux Etats membres, d'améliorations au niveau des soins de santé, et d'une demande accrue de services de soins de santé. Les fumeurs, mais aussi les non-fumeurs, les gouvernements et les employés devront supporter ces coûts. L'évidence empirique montre que la consommation de tabac constitue une charge nette venant grever les budgets nationaux, même en tenant compte des taxes perçues sur le tabac et des économies au niveau des dépenses de sécurité sociale dues à la mortalité prématurée chez les fumeurs.

Outre la taxe sur la valeur ajoutée (TVA), les Etats membres de l'UE imposent à la fois des taxes ad valorem et des accises spécifiques sur les produits du tabac. Le type d'accise influence sensiblement le montant de la taxe payée par paquet de cigarettes et c'est l'une des raisons qui explique les grandes différences de prix des cigarettes entre les Etats membres. Les accises spécifiques sont plus efficaces; elles sont plus faciles à administrer et soutiennent davantage les objectifs de santé publique de l'UE. En effet, elles découragent de la même façon la consommation de toutes les marques de cigarettes, au lieu d'encourager l'achat de marques moins coûteuses.

Le chapitre 2 explique pourquoi le niveau actuel de taxation du tabac dans les Etats membres de l'UE se situe en-dessous du niveau optimal en termes de génération potentielle de recettes. Le relèvement des taxes sur le tabac représente de loin la mesure la plus rentable en matière de lutte contre le tabagisme. Une taxation accrue permet en outre d'augmenter les recettes fiscales, même en cas de contrebande. Par ailleurs, le relèvement des taxes augmente le prix des cigarettes, qui n'est pas encore assez dissuasif pour la majorité des fumeurs de l'UE. Les mesures de lutte antitabac non basées sur le prix s'avèrent plus efficaces dans le cadre d'un programme global de lutte contre le tabagisme. Notons que même si la contrebande de cigarettes peut réduire l'impact escompté de l'augmentation des taxes – diminution de la consommation et hausse des recettes fiscales –, elle n'annulera jamais cet impact.

(...)

1. Recommandations organisationnelles et structurelles: investissements et capacité de réglementation.

- Les Etats membres et la CE doivent affirmer leur engagement en matière de lutte contre le tabagisme et leur volonté de réduire la morbidité et la mortalité liées au tabac en ratifiant et en mettant en œuvre le plus rapidement possible la CCLAT. Pour la mise en œuvre de cette convention-cadre, tous les Etats membres devront élaborer et mettre en œuvre des stratégies intégrées de lutte antitabac, axées à la fois sur la prévention, la protection, l'arrêt et la réduction des effets nocifs. La CCLAT devra être mise en œuvre selon les normes les plus strictes possibles compte tenu des limites constitutionnelles.
- La mise en œuvre de stratégies intégrées de lutte contre le tabac exigera d'investir beaucoup plus dans la lutte contre le tabac au sein de l'UE. Les données économiques indiquent que les actions de lutte contre le tabagisme viennent en deuxième place, juste après la vaccination des enfants, en termes de rentabilité des investissements. Aux Etats-Unis, les CDC ont recommandé des niveaux d'investissement de l'ordre de 4,8-12,73 € par habitant, niveaux à préconiser pour l'UE. Compte tenu des faibles niveaux de financement en matière de prévention du tabagisme dans les Etats membres, ceux-ci devraient augmenter immédiatement de 1-3 € les dépenses par habitant.

(...)

2. Recommandations concernant les actions spécifiques en matière de prévention du tabagisme.

2.1. Taxation

- Le relèvement régulier des taxes sur le tabac devrait faire implicitement partie des efforts des autorités européennes et nationales, étant donné que d'autres mesures de lutte contre le tabagisme s'appuient sur le renchérissement du tabac.
- Il convient d'harmoniser les niveaux de taxation sur la base de taux spécifiques, par opposition aux taxes dites *ad valorem*.
- Les taxes sur le tabac à rouler devraient également être revues à la hausse afin d'éviter le transfert vers ce type de produit du tabac.
- Le tabac devrait être retiré de l'indice des prix à la consommation.
- Il est nécessaire de renforcer la coopération internationale afin de mieux coordonner les politiques de taxation et de lutter efficacement contre la contrebande. La CE devrait élaborer une législation européenne sur la base de l'accord entre la Commission européenne, dix Etats membres et Philip Morris International (PMI) en matière de lutte contre le commerce illicite de cigarettes, contrefaites ou non.
- Parmi les priorités de l'UE devrait figurer une négociation précoce sur un protocole CCLT sur le commerce illicite, reprenant au minimum les dispositions de l'accord UE-PMI et de toute directive future basée sur ledit accord. Il est en effet nécessaire d'enrayer le manque à gagner considérable subi par les Etats membres et la Communauté suite à la contrebande internationale de tabac.

2.2. Publicité et promotion des ventes

- Tous les Etats membres qui ne l'ont pas encore fait doivent interdire complètement les publicités en faveur du tabac, y compris la publicité sur le lieu de vente, conformément aux dispositions de la ratification du CCLT.
- Cette interdiction devrait s'appliquer à toutes les formes de promotion des ventes de tabac. La proposition de règlement européen en matière de promotion des ventes en cours d'examen au sein du Parlement européen et du Conseil offre à cet effet un mécanisme approprié.

2.3. Débouchés du tabac

- La vente sur Internet de produits du tabac devrait être interdite, au même titre que la vente de produits du tabac dans les distributeurs automatiques.

(...)

2.4. Lieux de travail et lieux publics "non-fumeurs"

- L'UE et les Etats membres devraient suivre l'Agence de protection de l'environnement, le CIRC et les gouvernements finnois et allemand et classer le tabagisme passif parmi les agents carcinogènes professionnels.
- Une législation interdisant de fumer sur tous les lieux de travail aurait davantage d'impact si elle était promulguée à l'échelon européen. La législation développée en Irlande et en Norvège pourrait servir de modèle à une directive européenne.
- Une législation communautaire devrait être complétée par une législation au niveau des Etats membres, afin d'inclure les lieux publics qui ne sont pas des lieux de travail.

2.5. Stratégies de sevrage

- Tous les Etats membres qui ne l'ont pas encore fait doivent mettre au point des stratégies nationales pour le sevrage et le traitement du tabagisme. Celles-ci devraient inclure la formation de professionnels de soins de santé, le développement d'un réseau national de services de traitement et de sevrage tabagique, l'amélioration de l'accès aux traitements de substitution nicotinique et réduire des inégalités en matière d'offre de ces services.

2.6. Réglementation des produits du tabac

- Un nouveau cadre réglementaire global pour tous les produits à base de tabac et de nicotine doit être mis en place.
- Une information détaillée sur les caractéristiques physiques, chimiques et de fabrication de tous les produits du tabac devrait être rendue obligatoire et publique. Ces renseignements concerneraient, entre autres, le type de tabac utilisé, le type de traitement subi par le tabac, les ingrédients ajoutés, la composition du produit, les caractéristiques physiques et chimiques des émissions de tous les produits du tabac, la présence de nicotine et d'autres substances psychoactives, le mode de consommation et le comportement du consommateur.
- La directive 2001/37/CE devrait être améliorée avec l'intégration de la définition des ingrédients du Groupe d'étude de l'OMS sur la réglementation des produits du tabac.
- L'industrie du tabac est tenue de communiquer la totalité des additifs utilisés conformément aux termes et à l'esprit de la directive. Vu les risques élevés des produits du tabac, ces informations détaillées devront l'emporter sur le secret commercial.

LAP

examen
2^e sem.

Lundi 11/4/11
9h → 12h
J. 7000616

P1

MINISTÈRE DE LA JUSTICE - Direction de la protection judiciaire de la jeunesse

JLLM

CONCOURS POUR LE RECRUTEMENT DE :

DIRECTEURS DES SERVICES

DE LA PROTECTION JUDICIAIRE DE LA JEUNESSE

- 2007 -

sept jours
par M. Lemerica
Notes synthèses

CONCOURS EXTERNE ET INTERNE

Épreuve écrite d'admissibilité n°1 : Rédaction d'une note de synthèse établie à partir d'un ou plusieurs documents remis aux candidats.

(durée : 3 heures - coefficient 2)

NB : Il convient de ne faire figurer dans votre réponse aucune identification, aucun signe distinctif, ni sur la feuille principale ni sur les intercalaires éventuels (nom, initiales, signature, indications de lieux, de services, même fictifs, ...) conformément au principe d'anonymat. Toute copie remise en contradiction avec ces instructions est passible de nullité.

SUJET

Rédaction d'une note de synthèse établie à partir des documents suivants :

SOMMAIRE DES DOCUMENTS :

p. 2	Document n° 01	« Fil Santé Jeunes à l'écoute des ados » Bien-être et santé N° 234 – septembre 2006
p. 3	Document n° 02	Circulaire DGS/DGAS/DHOS/DPJJ 2002/282 du 3 mai 2002 relative à la prise en charge concertée des troubles psychiques des enfants et adolescents en grande difficulté. (extrait 1.1)
p. 4	Document n° 03	Rapport 2005 de l'Observatoire national de l'action sociale décentralisée – Protection de l'enfance
p. 6	Document n° 04	« La réalité du cannabis » Perspectives Sanitaires & Sociales – mai/juin 2005 – N° 180
p. 8	Document n° 05	« Faire de la santé un des leviers de l'action éducative » Actualités Sociales Hebdomadaires – 6 janvier 2006 – N° 2437
p. 10	Document n° 06	« L'enfant : la reconnaissance juridique d'un droit à l'autonomie » La santé de l'homme 367 – sept/oct 2003
p. 11	Document n° 07	« Protection de l'enfance – Les embarras de la médecine » Panorama du médecin – 18 septembre 2006 – N° 5028
p. 14	Document n° 08	« La Maison des adolescents – Un lieu d'écoute et d'accompagnement » Mutualistes N° 291
p. 16	Document n° 09	« L'obésité chez l'adolescent – S'adapter au sujet et mettre en confiance » Perspectives Sanitaires & Sociales – mai/juin 2005 – N° 180
p. 18	Document n° 10	« Répondre au mal-être des jeunes » La revue de la MEP – N° 154
p. 20	Document n° 11	« Accueillir et éviter les rechutes »
p. 21	Document n° 12	« 600 collégiens contre les leucodystrophies » Ouest France – 26 octobre 2006
p. 22	Document n° 13	« L'expression du mal-être des ados... » Lien social N° 772 – 03 novembre 2005
p. 23	Document n° 14	« Faire de la prévention mais dans quel but ? » ADOSEN N° 148 – juin 2005

FIL SANTÉ JEUNES À L'ÉCOUTE DES ADOS

Les données collectées sur le site web de Fil Santé Jeunes* (60 000 échanges sur différents forums + 15 000 mails adressés à l'équipe de 40 "écoutants" médecins, psychologues, conseillères conjugales et familiales, éducateurs, juristes) et analysées à l'occasion du 2^e Forum Adolescence, organisé en mai dernier par la Fondation Wyeth pour la santé de l'enfant et de l'adolescence, sont un reflet des préoccupations actuelles des ados. Les grands sujets qui les agitent sont, comme il fallait s'y attendre, la contraception, l'amour, les maladies sexuellement transmissibles, la question du corps et de sa transformation, mais aussi les dépendances (tabac, alcool, médicaments) et, pour une large part, le mal-être et les comportements à risque (dépression, troubles du comportement alimentaire, tentative de suicide).

* www.filsantejeunes.com Les jeunes peuvent aussi poser des questions et s'informer dans les domaines de la santé physique, psychologique et sociale en appelant au 0 800 235 236 tous les jours de 8 heures à minuit (appel anonyme et gratuit).

Circulaire DGS/DGAS/DHOS/DPJJ 2002/282
du 3 mai 2002

relative à la prise en charge concertée des troubles
psychiques des enfants et adolescents en grande
difficultés.

(extrait 1.1)

Le Haut comité de la santé publique souligne que si la mortalité est faible à l'adolescence, dans 70 % des cas il s'agit d'une mortalité violente et évitable. En effet, plus de la moitié des décès sont survenus par suite d'accidents et près d'un décès sur sept par suite d'une tentative de suicide. Dans une étude INSERM de 1998 auprès des adolescents de la protection judiciaire de la jeunesse, il était relevé que les conduites violentes dans l'année concernaient 50 % des garçons et 42 % des filles, que 41 % des garçons et 55 % des filles avaient été victimes de violences physiques et que 12 % des garçons et 49 % des filles avaient fait une tentative de suicide durant leur vie. Ces données suggèrent la prédominance des troubles psychosociaux à l'adolescence importants à analyser pour mieux les prévenir et ou les prendre en charge.

Les jeunes identifiés en grande difficulté, outre la souffrance psychique parfois intolérable dont leur comportement ou leur passage à l'acte témoignent, laissent les institutions démunies et nécessitent des prises en charge extrêmement complexes dont les résultats restent aléatoires. En effet, les parcours de vie de ces jeunes sont faits de ruptures successives que traduisent les échecs répétés des prises en charge - échec scolaire, exclusion des institutions, renvoi de la famille. L'adolescent difficile ne trouve pas de réponse adéquate dans le cadre de son environnement qu'il met en tension ou en échec, induisant de ce fait des attitudes de ruptures et de rejet et le renvoi sur d'autres filières de prise en charge, souhaitées plus « contenant ».

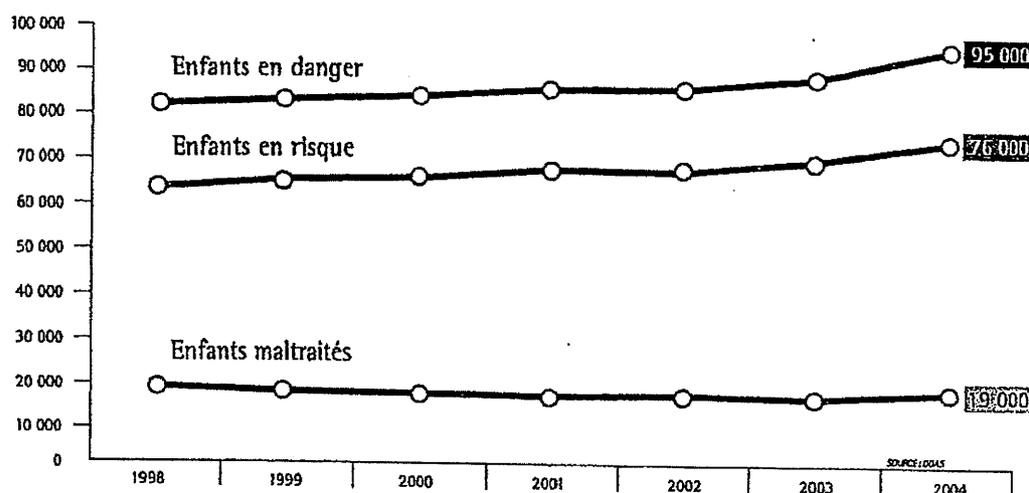
Afin de mieux connaître ces publics pour agir avec pertinence, il importe de mettre en commun les données disponibles, de développer et d'actualiser études et recherches sur ce thème.

RAPPORT 2005

I. L'ACCROISSEMENT CONSTANT DU RISQUE

La progression inquiétante de l'année 2004 nécessite d'être appréhendée plus finement. Parmi les enfants en danger, on distingue les enfants maltraités et les enfants en risque². C'est encore une fois la progression du nombre d'enfants en risque qui explique la progression globale. Toutefois on constate pour la première fois une évolution de la maltraitance.

L'évolution du nombre d'enfants en danger par type de danger

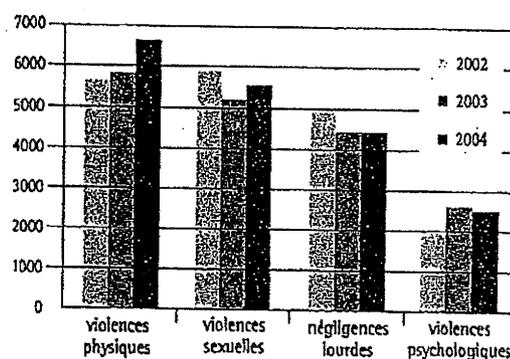


I. 1. Les enfants maltraités

En effet, le nombre d'enfants maltraités progresse (+ 1000 enfants), et plus particulièrement celui des enfants victimes de violences physiques (+ 800).

L'évolution du nombre d'enfants maltraités par types de mauvais traitements entre 2002 et 2004

	2002	2003	2004
Violences physiques	5 600	5 800	6 400
Violences sexuelles	5 900	5 200	5 500
Négligences lourdes	5 000	4 400	4 700
Violences psychologiques	2 000	2 600	2 500
Total enfants maltraités	18 500	18 000	19 000



Selon les explications qualitatives données par les départements, cette évolution traduirait une progression de la violence dans les relations sociales³. On a le sentiment

d'une société de plus en plus déstabilisée dans les règles élémentaires du vivre-ensemble. C'est également probable pour les abus sexuels qui progressent aussi.

² Conformément aux définitions du Guide méthodologique de l'ODAS (juin 2001) :

- un enfant maltraité est un enfant victime de violences physiques, d'abus sexuels, de violences psychologiques, de négligences lourdes, ayant des conséquences graves sur son développement physique et psychologique.
- un enfant en risque est un enfant qui connaît des conditions d'existence risquant de compromettre sa santé, sa sécurité, sa moralité, son éducation ou son entretien, sans pour autant être maltraité.
- C'est l'ensemble de ces enfants que recouvre la notion d'enfants en danger.

³ Ce constat peut être rapproché d'informations recueillies par ailleurs sur la vie des établissements d'aide sociale à l'enfance selon lesquelles les enfants accueillis seraient de plus en plus violents.

I. 2. Les enfants en risque

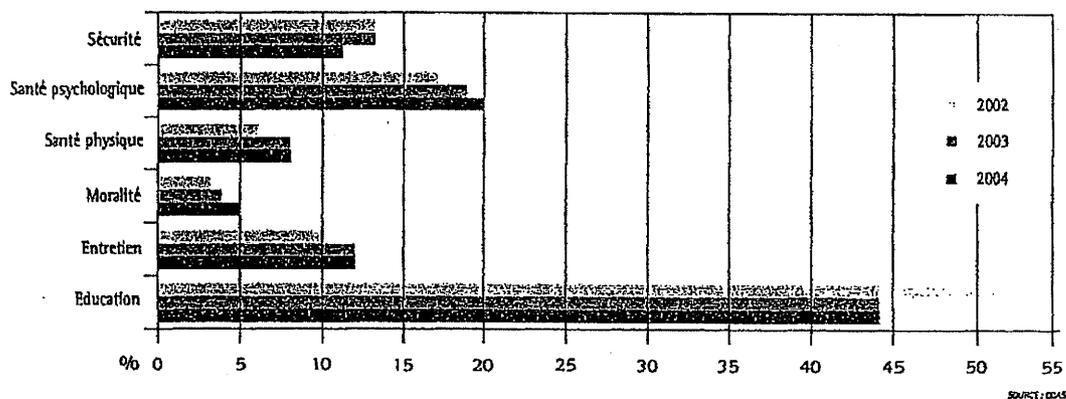
Depuis plusieurs années, le nombre d'enfants en risque progressait régulièrement mais lentement. Cette année la progression est très forte (+ 5000 enfants). Dans ce genre de situation, l'enfant n'est pas maltraité mais il vit dans un contexte familial particulièrement dégradé qui menace son développement sur le plan éducatif et/ou matériel. Cela marque donc une accélération du processus de déstabilisation des familles par rapport aux années précédentes, expliquant pour partie le désarroi des travailleurs sociaux qui continuent de transmettre plus de la moitié des signalements pour risque à la Justice (52% en 2004 contre 51% en 2003).

En revanche, la répartition par type de risque est stable. C'est le risque de nature éducative qui s'affirme

comme très largement prépondérant : il est mentionné comme risque principal dans 44% des cas. Il signifie que l'enfant est confronté à des problèmes aigus de scolarisation et de socialisation qui compromettent fortement ses chances d'intégration. Si l'on ajoute les enfants signalés parce qu'il existe un risque pour leur santé psychologique voire pour leur moralité ce sont 69 % donc 2/3 des enfants en risque qui sont concernés.

Les autres risques, plus directement liés à une dégradation des conditions matérielles de vie s'affirment comme minoritaires. En revanche ils sont plus préjudiciables à court terme. C'est pourquoi on peut penser que seuls ces risques devraient conduire à un signalement judiciairisé, et au-delà à un placement en cas de désaccord avec la famille.

Les types de risque cités à titres principal en 2002, 2003 et 2004



II. L'IMPACT DE L'ISOLEMENT

L'analyse des facteurs de danger consiste à identifier ce qui, dans le mode de vie de l'enfant, a été repéré par

les travailleurs sociaux comme cause(s) du danger, qu'il s'agisse d'enfants maltraités ou d'enfants en risque. La structure de l'ensemble des facteurs de danger est stable depuis 3 ans qu'elle est observée.

Facteurs à l'origine du danger	Nombre d'enfants concernés par le facteur	
Carences éducatives des parents	27 800	soit 50% des enfants signalés
Conflits de couple et séparation	23 600	soit 40% des enfants signalés
Problèmes psycho pathologiques des parents	12 350	soit 23% des enfants signalés
Dépendance à l'alcool ou à la drogue	11 400	soit 21% des enfants signalés
Maladie, décès d'un parents, chocs affectifs	5 350	soit 10% des enfants signalés
Chômage, difficultés financières	12 350	soit 23% des enfants signalés
Cadre de vie, habitat	4 000	soit 8% des enfants signalés
Errance, marginalité	3 800	soit 7% des enfants signalés
Autres	11 400	soit 21% des enfants signalés

SOURCE: DGAS

La réalité du cannabis



La consommation de cannabis a nettement augmenté depuis 10 ans, particulièrement chez les jeunes. Chez les garçons de 17 ans, l'expérimentation a doublé en 10 ans et la consommation répétée a triplé. On compte en France 850 000 consommateurs réguliers de cannabis, dont 450 000 quotidiens, principalement des jeunes. Par ailleurs, l'âge de l'expérimentation est de plus en plus précoce.

La France est l'un des pays d'Europe où le niveau de consommation est le plus élevé.

La perte de motivation et de confiance en soi peut être une conséquence de la consommation régulière de cannabis. Elle va concerner les activités scolaires, les loisirs mais aussi les relations amicales ou familiales.

Certains adolescents commencent à fumer pour apaiser une souffrance, mettre à distance des problèmes scolaires, familiaux ou personnels et, petit à petit, un "cercle vicieux" s'installe. Les problèmes ne sont pas pour autant résolus mais le cannabis permet seulement de les masquer, les relations sont restreintes et le jeune s'enferme sur lui-même.

L'usage régulier se transforme alors en habitude de vie. La recherche de cannabis, de lieux et d'occasions où on peut en fumer devient une obsession. La dépendance s'installe progressivement. Elle est essentiellement psychologique. Alors que certaines personnes s'arrêtent de fumer très facilement, les personnes dépendantes sous-estiment souvent leur dépendance au cannabis et ne pourront s'en passer sans une aide médicale.

Pour certains, les effets du cannabis, le plaisir et la détente qu'il procure suffisent à occuper la vie. On se sent bien sans rien faire. Un cercle vicieux peut s'installer rapidement.

Le cannabis met en péril les études

Il est clairement établi que le cannabis diminue les capacités de mémoire immédiate, de concentration, de vigilance et d'attention chez les jeunes usagers et entraîne donc souvent de sérieuses difficultés scolaires.

L'adolescent ne trouve plus d'intérêt dans ce qu'il entreprend et ne se donne donc plus les moyens de réussir ses objectifs. La dégradation peut être rapide et le retard s'accumule donc simplement et rapidement.

Le cannabis et ses mauvaises surprises

"Quand on fume trop" ou dans certaines circonstances, "par exemple, quand on a aussi bu de l'alcool, quand on est fatigué ou angoissé, on peut faire un bad trip", intoxication aiguë qui se manifeste par un malaise physique et ou psychologique. Le jeune ressent un mal physique, des tremblements, du mal à respirer, des palpitations. Certaines personnes vont vomir et même perdre connaissance des hallucinations peuvent se faire ressentir.

Perspectives Sanitaires et Sociales a interrogé Aurélien Connan, psychologue social de santé à Marseille, sur l'enquête conduite auprès de 365 jeunes marseillais. En effet, 365 jeunes mar-

seillais de 11,6 ans en moyenne ont été interrogés dans 4 écoles élémentaires et 3 collèges. Trois variables sont alors prises en compte : le sexe, le niveau scolaire (CM2, 6^e ou 5^e) et le milieu social (établissement scolaire classé en Zone d'Education Prioritaire ou non). Afin de connaître leurs représentations sur le cannabis (opinions, croyances et informations que partagent les membres d'un groupe donné), deux techniques qualitatives sont utilisées : l'une individuelle (associations libres) et l'autre collective (focus-groupes). Les informations recueillies sont traitées avec le logiciel "Alceste" et une analyse thématique manuelle est réalisée afin d'analyser les discours issus de 25 focus-groupes.

Pour le psychologue social, le cannabis est un objet normalisé et investi d'enjeux sociaux particuliers.

L'expansion et la banalisation du cannabis ne font plus de celui-ci un objet transgressif. Au contraire, fumer du cannabis est considéré aujourd'hui par une majorité de jeunes comme

La consommation régulière de produits illicites et licites à 17/18 ans

	Filles	Garçons	Ensemble
Alcool	7,5 %	21 %	14,4 %
Tabac	39,9 %	40,2 %	40 %
Cannabis	7,6 %	17,9 %	12,9 %
Médicaments psychotropes	4,7 %	1,3 %	2,9 %

Source : Conseils Aide et Action contre la Toxicomanie

un comportement normatif qui garantit même dans certains cas l'insertion dans un groupe "Pour faire comme les autres", "Comme les rappeurs", "C'est une mode", etc. Le premier joint, tel un rite de passage, permet au jeune de s'intégrer au groupe ou d'y être reconnu "Il fume du shit pour s'intégrer", "Pour frimer", "Il lui dit : si tu fumes, tu deviendras un homme, alors il fume pour montrer qu'il est grand", etc.

La peur de l'exclusion et le besoin de se conformer à l'autre et aux attentes du groupe prennent une place importante dans l'univers représentationnel du cannabis chez les jeunes. L'influence des pairs est, en effet, considérée comme la cause première des expérimentations : à l'adolescence, la comparaison sociale et le regard de l'autre sont des éléments qui prennent un sens majeur dans la construction de l'estime de soi et de l'identité. En effet, à l'adolescence, les jeunes sortent progressivement de la sphère d'influence parentale au profit de celle des pairs et se retrouvent dans des situations de proximité plus accrues avec le cannabis.

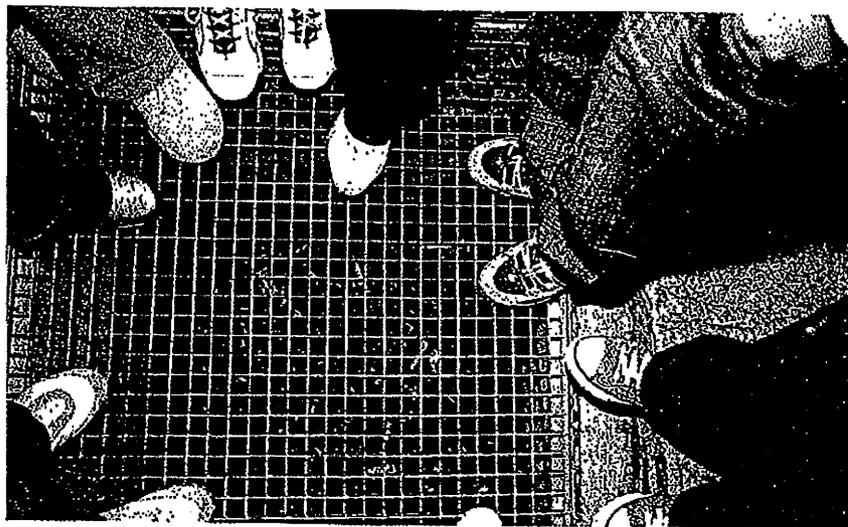
Pour les adolescents, ce sont avant tout les attentes perçues de la part de l'environnement, plutôt que les qualités attribuées au cannabis ou leurs propres goûts et jugements qui déterminent essentiellement les intentions comportementales de consommation. Il s'agit, en effet, de faire comme les autres ou, pour les plus jeunes, de faire comme les grands. Pour beaucoup, le cannabis permet d'acquérir un statut social particulier, il permet de frimer, de faire le grand, mais aussi d'attirer les filles. Il remplace même dans certains discours l'autre manquant "Le shit, c'est un peu son animal de compagnie", "C'est un ami" ...

Alors que faire ?

Certains établissements dont l'ASM 13 mettent en place des journées d'information pour les jeunes de la région et afin que les médecins présents puissent répondre à toutes leurs interrogations.

L'enquête conduite à Marseille a mis en évidence chez les jeunes un besoin considérable d'expression et de dialogue avec l'adulte autour du cannabis et des autres produits psychoactifs. Dans un premier temps, il demeure essentiel de les laisser s'exprimer hors de toute instance moralisatrice ou directive.

Ensuite, il apparaît important de donner à l'enfant une information claire et cohérente dès l'école élémentaire afin qu'il puisse se posi-



tionner par rapport aux produits psychoactifs et faire face aux sollicitations qu'il peut rencontrer. Néanmoins, on sait que la seule information ne suffit pas à la modification des comportements : la prévention doit pouvoir s'instaurer dans une dynamique de communication entre pairs, avec les adultes et surtout dans les institutions qu'ils fréquentent.

Face à l'ampleur du phénomène et à l'écart entre l'image du cannabis et sa réalité, il est nécessaire d'informer et d'aider les jeunes consommateurs en difficulté et leur entourage. Dans le cadre du plan gouvernemental de lutte contre les drogues illicites, le tabac et l'alcool 2004/2008, le ministère des Solidarités, de la Santé et de la Famille, la Mission interministérielle de lutte contre la drogue et la toxicomanie (Mildt) et l'Institut National de Prévention et d'Education pour la Santé (INPES) mettent en place un programme de prévention sur l'usage du cannabis. Une ligne spécifique, "Ecoute cannabis" : 0 811 91 20 20, est mise en place pour répondre aux questions, tous les jours de 8 à 20 h, coût d'une communication locale depuis un poste fixe.

220 centres de consultation cannabis, gratuits et anonymes, ont été mis en place dans certains départements. Les jeunes qui le désirent sont reçus par des spécialistes évaluant ainsi leur situation face au cannabis : une écoute, des informations personnalisées et des solutions adaptées leurs sont alors proposées. Toutes ces consultations sont ouvertes à l'entourage de l'adolescent.

Pour Aurélien Connan, les programmes de prévention doivent notamment permettre le développement ou l'amélioration de l'estime de soi, de l'esprit critique et des habiletés sociales, mais aussi apporter des ressources visant l'adoption de copings adaptés lors de situa-

tions de crise. Concrètement, c'est dans le dialogue et la mobilisation des ressources collectives dès le plus jeune âge et l'utilisation de techniques projectives que les stratégies préventives doivent trouver leur sens, et non dans des actions focalisées sur les substances et l'exposé de leurs dangers. En fin de compte, il ne s'agit aucunement d'imposer aux jeunes un modèle auquel s'identifier de manière aveugle ou une norme de comportement à laquelle se conformer sans tenir compte de leur personnalité ou des caractéristiques de leur environnement.

Une campagne médiatique a été lancée au mois de février dernier, sous forme de 6 films diffusés à la télévision, 8 spots à la radio ainsi que des messages dans la presse nationale. Des jeunes se sont mis en scène pour témoigner des risques encourus, la mise en péril de la scolarité, la perturbation des relations affectives et la dépendance au produit et l'intoxication aiguë.

La consommation de substances illicites par les jeunes est devenue une priorité gouvernementale. ■

Emmanuelle de Vaublanc
avec la contribution d'Aurélien Connan

Sources : Guides établis par :

- le ministère des Solidarités, de la Santé et de la Famille
- La Mission Interministérielle de lutte contre la drogue et la toxicomanie
- L'Institut de Prévention et d'Education pour la Santé

Pour plus d'informations
www.drogues.gouv.fr
www.inpes.sante.fr
www.filsantejeunes.com

Protection judiciaire de la jeunesse

Faire de la santé un des leviers de l'action éducative

Afin de mieux prendre en compte la santé des jeunes suivis en s'appuyant sur les évolutions législatives et les dernières données de l'Inserm, la direction de la protection judiciaire de la jeunesse a réactualisé sa stratégie d'action. S'inspirant de diverses expériences de terrain, elle recommande aux professionnels de saisir toutes les opportunités offertes par l'action éducative et de renforcer la pluridisciplinarité.

« La politique de santé à l'égard des jeunes confiés à la direction de la protection judiciaire de la jeunesse (PJJ) est au cœur de notre stratégie de prise en charge éducative, c'est l'un de ses tenants mais aussi de ses aboutissants. Mieux prendre en compte la santé du jeune, faire évoluer son rapport au corps, faire que, là aussi, il aille mieux, c'est pleinement faire œuvre d'éducation », affirmait Michel Duvette, directeur de la PJJ, lors du « Regroupement national politique de santé à la protection judiciaire de la jeunesse » (1). A cette fin, « toutes les opportunités pour faire durablement évoluer les pratiques » doivent être saisies.

La politique de santé s'est structurée à la PJJ en 1999 autour d'une approche de santé publique reposant sur trois axes : participer aux politiques publiques, intégrer la santé – « état de complet bien-être physique, mental et social », selon l'Organisation mondiale de la santé – dans l'action éducative et développer un travail clinique et épidémiologique. Depuis, les lois du 2 janvier 2002 renouant l'action sociale et médico-sociale et de santé publique du 9 août 2004 ont dessiné un nouveau paysage qui, selon le directeur, « oblige à revisiter les fondamentaux de l'action éducative ». Un paysage dont les contours sont également remodelés par les résultats de l'enquête « Santé des 14-20 ans de la protection judiciaire de la jeunesse (secteur public), sept ans après » de l'Inserm (voir encadré page 38). Autant d'évolutions qu'a voulu intégrer la stratégie d'action en santé élaborée jusqu'en 2008 par la PJJ (voir encadré ci-contre).

(1) Organisé les 18 et 19 octobre 2005 au Centre national de formation et d'études (CNFE), à Vaucluse.

Sur le terrain, c'est autour de la « triade besoin-demande-réponse », selon Jocelyne Grousset, médecin en charge du dossier de santé publique, que doit s'articuler l'action. Première démarche donc, l'exploration des besoins. Le moment de l'arrivée du jeune doit être, selon elle, un temps propice pour aborder ses besoins immédiats (début ou poursuite d'un traitement, couverture sociale...) et recueillir son point de vue sur sa santé comme celui de ses parents. Mais la démarche doit se poursuivre tout au long du suivi éducatif grâce à la disponibilité et à l'écoute des équipes et à leur capacité à passer le relais. « Chaque professionnel doit s'approprier certains domaines de la santé et trouver un mode de communication pour faciliter les échanges et la circulation de l'information », affirme le médecin.

La détermination des besoins peut s'appuyer également sur les enseignements des enquêtes épidémiologiques. Ainsi, celle de l'Inserm met en évidence les liens existant entre les troubles du sommeil et les difficultés sociales et scolaires ou les tentatives de suicide. « La perturbation chronique du sommeil est donc une bonne porte d'entrée pour repérer les jeunes qui vont plus mal que les autres », analyse Jocelyne Grousset. Susciter l'expression collective des jeunes permet aussi de repérer leurs besoins. Dans les centres de placement immédiat du Rhône, les équipes éducatives et l'infirmière départementale organisent ainsi des soirées « santé », où, en groupe, les mineurs peuvent s'informer et prendre la parole.

Autre expression à provoquer : celle des professionnels pour connaître leurs constats et difficultés. C'est à partir de leurs opinions que la direction départementale de la protection judiciaire de la jeunesse a défini une politique de santé dans les Bouches-du-Rhône. « Pour dresser un état des lieux, les infirmières ont interrogé tous les directeurs de service et les équipes, à l'aide d'un questionnaire établi avec le comité d'éducation pour la santé. ... »

LES ORIENTATIONS JUSQU'EN 2008

La stratégie d'action en santé 2005-2008 de la protection judiciaire de la jeunesse (PJJ), qui doit être déclinée sur les territoires, repose principalement sur :

- ♦ l'adoption d'une approche adaptée au public de la PJJ, dans les domaines de l'adolescence et de la vie affective et sexuelle, de l'accès aux soins et à la prévention, de la prise en charge des troubles psychiques et de la réduction des comportements de consommation de psychotropes ;
- ♦ le développement de pratiques professionnelles en santé par l'activation des commissions santé et la valorisation d'outils ;
- ♦ la mise en conformité des pratiques selon les dispositions de la loi du 2 janvier 2002 (intégration des modalités de prise en charge de la santé dans le livret d'accueil et le règlement de fonctionnement, recommandations de bonnes pratiques...) ;
- ♦ la participation à la programmation établie par la loi du 9 août 2004 (contribuer au diagnostic de santé de la population, collaborer au groupement régional de santé publique ou au comité des programmes régionaux, veiller à la prise en compte des besoins du public de la PJJ...) ;
- ♦ l'inscription d'un volet santé au sein des dispositifs de formation.

... Etaient abordés les collaborations avec le milieu médical, l'accès aux droits, le dépistage des troubles psychologiques... », explique Béatrice Tribonté, directrice chargée du dossier santé à la direction départementale de la PJJ. Un groupe de travail, formé de professionnels divers œuvrant aussi bien en milieu ouvert que dans le secteur de l'hébergement ou des services éducatifs auprès des tribunaux, a alors dégagé des axes à développer.

Sonder la demande du jeune est en outre indispensable pour le rendre acteur de sa santé. Cette demande peut prendre des formes variables : consultation, information, dialogue... Elle peut aussi ne pas exister. Du moins en apparence. Ou être en décalage avec ce qu'appréhendent les adultes. « La santé signifie davantage pour les adolescents le bien-être au quotidien. Un jeune dira qu'il est en bonne santé s'il se sent en harmonie avec son environnement », observe Marie Choquet, directrice de recherche à l'Inserm, qui a mené l'enquête PJJ. « De plus, les jeunes ne conçoivent pas la santé comme évolutive mais plutôt comme dépendante de facteurs extérieurs », précise Jocelyne Grousset. En outre, il ne faut pas oublier que notre intervention est en général ressentie par le jeune et sa famille comme une intrusion car effectuée sous la contrainte. »

Aussi, pour favoriser l'adhésion à la démarche, faut-il, outre travailler avec les familles, « aller au-devant de celui qui ne semble pas formuler de demande ». L'expérience menée à la maison d'arrêt de Dijon en est une illustration. L'infirmière de la PJJ, Annie Robert, rencontre en entretien individuel tous les jeunes entrant en prison, puis essaie de les revoir. Elle les questionne sur ce que signifie pour eux être en forme et aborde des sujets aussi divers que la scolarité, l'hygiène, les vaccinations, leurs relations avec les autres, l'alimentation, les conduites addictives. « Le but, résume-t-elle, est d'atteindre chez l'adolescent une zone de conscience pour qu'il se projette sur un terrain sain et que les équipes éducatives puissent ensuite s'en emparer. » Et de constater :

(1) Voir ASH n° 2036 du 12-09-97, p. 21.

« Plusieurs mineurs ont rebondi à leur sortie sur les permanences "santé" des structures de la PJJ. »

Aller au-devant de la demande des adolescents implique aussi de susciter le dialogue sur leur vie affective et sexuelle au cœur de leurs préoccupations. Il s'agit alors de ne pas se cantonner à la prévention des risques (infections sexuellement transmissibles et grossesses), mais

de tenir compte de ce qui se joue : questionnement sur l'identité et sens de la relation à l'autre. C'est dans cette optique qu'en 1983 a été créé, à Saint-Denis, l'Espace vie adolescence (EVA) (1). Service éducatif pluridisciplinaire pour adolescentes, EVA fonctionne sans ordonnance judiciaire et accueille en son sein des partenaires tel que le Mouvement français pour le planning familial. « C'est un lieu préservé dont l'accès est gratuit, anonyme et volontaire, et où nous proposons un accueil, une écoute et un accompagnement. Y est pris en compte ce qui s'exprime sous les manifestations du corps et de la sexualité à l'adolescence », résume son chef de service, Chantal Perotet. Les adolescentes reçues ont souvent vécu des ruptures affectives précoces, des prises de risque, des errances, des violences sexuelles, des mutilations... EVA réfléchit aussi à la création d'outils dédiés aux jeunes hommes. Ailleurs, en Rhône-Alpes, toujours dans l'idée de favoriser le dialogue sur la vie affective et sexuelle, des éducateurs ont bénéficié, à leur demande, de formations leur permettant d'aborder ce thème et de monter des projets.

Différentes stratégies, comme les bilans de santé ou les actions d'éducation pour la santé, peuvent être activées pour stimuler la demande du jeune, voire l'aider à prendre conscience de l'existence d'un problème. Plusieurs initiatives sont d'ores et déjà menées en ce sens. A la maison d'arrêt de Besançon, des actions collectives de prévention et de réduction des risques sont ainsi proposées aux mineurs, souvent impliqués dans des délits en lien avec des psychotropes. L'infirmière de la PJJ et une assistante sociale de l'association Solea y animent des séquences sur le cannabis, l'alcool et le tabac afin d'inciter

les jeunes à réfléchir sur leurs représentations de l'usage de produits et, au-delà, à se décider à engager une prise en charge. Dans le Finistère, le travail sur les conduites à risques, nécessaire au vu du nombre d'accidents sur la voie publique impliquant des jeunes, passe par une formation aux premiers secours et à la gestion des risques, validée officiellement. « Cette action menée en partenariat avec la mission locale est un levier pour s'interroger sur sa santé, via les thèmes inévitablement abordés (alcool, drogue, médicaments, VIH, hygiène, vaccinations...) et sur son rapport aux autres », analyse Philippe Rousselot, infirmier et moniteur de secourisme.

La construction d'une réponse adaptée induit le rapprochement des professionnels du soin, de la prévention et de l'éducation. « Il est important, rappelle Jocelyne Grousset, de mettre en commun des approches différentes, sources de décloisonnements et d'échanges, et primordial d'explorer, au niveau des services comme du département, les ressources et les partenaires potentiels. » C'est d'ailleurs en participant au « Réseau autour d'Avicenne » (du nom de l'hôpital de Bobigny) que le centre d'action éducative (CAE) de Pantin a appris la création d'une maison des adolescents et qu'il a pu s'y impliquer. Afin de faciliter l'entrée dans le parcours de soin de jeunes en grande difficulté, pour lesquels une réponse spécifique et concertée était nécessaire, des éducateurs du CAE y interviennent depuis un an. Une convention devrait bientôt sceller le partenariat. « Nous espérons que cela permettra de faire valoir la compétence des personnels éducatifs dans ce travail d'accompagnement et de prévention des conduites à risques en particulier », remarque Fabrice Chauvet, éducateur.

Pour mettre en œuvre des actions et articuler les interventions, les services sont également invités à faire appel aux commissions santé. Instances d'animation de la politique de santé à la PJJ sous l'autorité du directeur territorial, elles rassemblent la large palette des professionnels concernés ainsi que des partenaires extérieurs. Et offrent un cadre général aux acteurs de la santé et de l'éducatif qui peinent parfois à collaborer.

Florence Raynal

L'enfant : la reconnaissance juridique d'un droit à l'autonomie

Depuis trente ans, demander son avis à l'enfant est devenu la norme, dès lors que la volonté du mineur apparaît éclairée. En matière de dépistage du sida - gratuit et anonyme dans les centres de planning familial - et de contraception, le mineur jouit d'ailleurs d'une autonomie reconnue. La pratique révèle toutefois combien, faute d'une " majorité spéciale au contrat de soins ", les mineurs résidant en France peuvent difficilement s'adresser seuls à des médecins (9). La reconnaissance du droit d'autonomie peut par ailleurs être source de contradictions en plaçant les parents face à un dilemme : doivent-ils protéger leur enfant au détriment de la conquête de son autonomie ou doivent-ils favoriser l'épanouissement de l'autonomie de l'enfant au péril de sa santé, éventuellement ? La question se pose avec une acuité dramatique quand sont en jeu des conduites à risques, généralement pratiquées par les jeunes avec les pairs. Ce dilemme s'exprime plus largement hors du champ sanitaire et renvoie à une ambivalence structurelle qui déchire les parents contemporains, invités à en faire beaucoup pour leurs enfants, mais pas trop non plus, bref à avoir du " talent ", comme le dit le philosophe Alain Renaut (10). On aurait envie d'ajouter que ces parents sont invités à avoir la santé pour résister à de telles pressions ! Au-delà de la boutade, on peut penser que l'action éducative parentale est pour partie conditionnée par la santé des parents eux-mêmes et qu'une réflexion sur la santé des enfants ne peut, de fait, faire l'économie d'une réflexion sur celle des parents : des unités mères-enfants ont été créées dans certains hôpitaux pour aider des jeunes femmes à prendre en charge leurs bébés alors qu'elles souffrent elles-mêmes de toxicomanie ou d'une pathologie psychique. Sur ce point, la question de l'éducation à la santé comme élément de la fonction parentale croise tristement celle des inégalités sociales face à la santé et, aussi, face à la mortalité.

(9) Cf. Rubellin-Devichi J., op. cit., p. 691.

(10) Renaut A., Manent P. La question de l'autorité : modernisation du lien familial ?, Comprendre, n° 2, Le lien familial, 2001 : 185-206.

Parce que la santé n'a pas de prix, on ne peut que soutenir l'éducation à la santé des enfants et des adultes, des hommes comme des femmes. Chaque famille peut y contribuer, y compris en essayant de faire plaisir à sa progéniture tout en transmettant un message. En lisant ou relisant les désormais célèbres aventures de Harry Potter, chaque enfant (re)découvre que même son héros fréquente régulièrement l'infirmier scolaire, quand il ne suit pas les enseignements du professeur Chourave sur les propriétés curatives de la mandragore. La santé, ça s'apprend ! Et ça s'entretient !

Enquête



Protection de l'enfance Les embarras de

Signalements de maltraitance : les failles du système

Difficulté pour les libéraux d'effectuer des signalements, mauvaise collaboration entre les différents acteurs... Autant de dysfonctionnements auxquels devra remédier la réforme élaborée par le ministre de la Famille.

Il aura fallu toutes ces « affaires » pour que la réforme de la protection de l'enfance s'impose comme une évidence. Celle d'Outreau d'abord. Un fiasco judiciaire. Drancy, ensuite. En août 2004, on découvrait cinq enfants de 13 mois à sept ans, nus, sous-alimentés, dans un appartement jonché d'immondices et d'excréments. Angers, enfin. Un procès de pédophilie impliquant 65 personnes, de mars à juillet 2005.

Selon Philippe Bas, ministre délégué à la Sécurité sociale, aux Personnes âgées, aux Personnes handicapées et à la Famille, ces tragédies ne sont pourtant que « la partie émergée de l'iceberg. Car il y a tous ces enfants qui souffrent en secret et dont le nombre ne cesse de croître ». Plus de 270 000 sont pris en charge par les services de l'aide sociale à l'enfance.

Aujourd'hui, une proposition de loi est en

discussion au Parlement. Elle devrait « renforcer la prévention, organiser le signalement et diversifier les modes de prise en charge des enfants ». Avec comme « chef de file de la protection de l'enfance dans le département », le conseil général.

95 000 SIGNALEMENTS EN 2004

Pour le moment, cette réforme fait plutôt l'objet d'un consensus entre les différents



la médecine

Qu'il s'agisse du signalement des cas de maltraitance et des sévices sexuels ou du débat sur le dépistage et le traitement des troubles du comportement, la protection de l'enfance place souvent le corps médical dans une situation inconfortable

acteurs de la santé et de la petite enfance. Philippe Bas se réjouit d'ailleurs de la « forte convergence des points de vue ». De quoi rendre jaloux son confrère de l'Intérieur, Nicolas Sarkozy, dont le projet de loi sur la prévention de la délinquance lui, est loin de faire l'unanimité.

La réforme de Philippe Bas va intervenir alors que les signalements d'enfants établis par les conseils généraux sont en hausse : 95 000 en 2004, soit 7 % de plus que l'année précédente selon l'Observatoire national de l'action sociale décentralisée (Odas).

Bien sûr, ces enfants « en danger » ne sont pas tous dans une situation comparable. 76 000 d'entre eux sont considérés comme « en risque » en raison de leurs conditions d'existence, qui menacent de compromettre leur santé, leur sécurité, leur moralité, leur éducation ou leur entretien, sans pour autant être maltraités, explique l'Odas.

Les enfants véritablement « maltraités » - 19 000 - sont ceux victimes de violences physiques, d'abus sexuels, de violences

psychologiques ou de négligences lourdes ayant des conséquences graves sur leur développement physique et psychologique.

Face à ces jeunes victimes, l'Odas conseille de revoir les méthodes d'action, notamment en privilégiant la protection administrative décentralisée (l'aide sociale à l'enfance [ASE] sous l'égide du conseil général) par rapport à la protection judiciaire. Car le recours à la justice est considéré comme plus stigmatisant pour l'enfant et conduit à une méfiance des familles vis-à-vis des travailleurs sociaux, constate l'Odas. Sans compter que cela représente « une surcharge de travail pour les magistrats, ce qui entraîne une augmentation des délais de traitement, préjudiciable au final à l'enfant ».

Et pourtant, regrette l'Odas, « on observe aujourd'hui une augmentation du taux de judiciarisation des signalements ». Près de six dossiers sur dix continuent à être transmis à la justice.

Des « excès » que pourrait éviter une meilleure collaboration entre les différents

intervenants. Car « la circulation entre les différents acteurs est encore insuffisante, note l'Odas. C'est le cas, notamment, entre la justice et l'ASE en ce qui concerne les signalements ».

Selon le Conseil national de l'Ordre des médecins (Cnam), en 2004, seulement 10 % des cas de maltraitance à enfant faisaient l'objet d'un signalement. Tous ne sont pas effectués par des médecins, mais ceux-ci sont souvent au premier rang pour repérer les enfants en danger. Notamment les médecins scolaires.

L'article 44 du code de déontologie médicale oblige d'ailleurs tout médecin qui « discerne qu'une personne auprès de laquelle il est appelé est victime de sévices ou de privations » à « mettre en œuvre les moyens les plus adéquats pour la protéger ». Le tout en faisant preuve de « prudence et de circonspection ».

Dans les faits, cette prudence peut s'avérer presque paralysante pour beaucoup de professionnels. « C'est très difficile pour un

Enquête



Protection de l'enfance : les embarras de la médecine

❶ *médecin libéral de faire un signalement* », reconnaît Irène Kahn-Bensaude, membre du Cnom et elle-même pédiatre. « S'il prend cette décision, il se met à dos la famille. Non seulement celle-ci lui en voudra, mais en plus, elle risquera de déménager. Sans compter que quand cela se passe dans un village, tout finit toujours par se savoir... ».

Voilà pourquoi, regrette-t-elle, « beaucoup de généralistes refusent de faire le signalement eux-mêmes ».

Ce qui ne signifie évidemment pas que les enfants sont abandonnés dans leur détresse. « Une solution consiste à les envoyer à l'hôpital, où les pédiatres ou les pédopsychiatres effectueront eux-mêmes le signalement », indique Irène Kahn-Bensaude.

Annie Laffont, pédiatre à Rodez, témoigne à son tour. « La première fois que j'ai eu à faire un signalement, j'ai rencontré beaucoup de problèmes, avec les services sociaux comme avec les services judiciaires, qui n'ont

pas tenu compte de ce que j'avais observé. Peut-être ont-ils mal interprété. Le fait est que tout cela s'est retourné contre la famille, contre l'enfant et contre moi-même. » Résultat : elle ne signe plus elle-même les certificats et confie les patients qui lui inspirent de l'inquiétude au service pédiatrie de l'hôpital.

Et après tous ces efforts, il faut encore batailler pour savoir ce que devient l'enfant. Car « il n'y a aucun retour vers les médecins libéraux », déplore Irène Kahn-Bensaude. J'ai fait plusieurs signalements, sans que jamais le procureur ne me donne de nouvelles ».

Bref, une collaboration insuffisante quand elle n'est pas inexistante. « Il existe un cloisonnement professionnel tel que chacun garde pour lui sa parcelle de secret en estimant que les autres ne sont pas à même de la partager », déclarait dans nos colonnes (n° 5025 du 10 juillet 2006) Valérie Péresse, députée UMP et auteure d'une proposition de loi sur les droits de l'enfant. D'où l'idée d'instaurer un « secret partagé » sur le modèle du secret médical.

Inutile, estime Irène Kahn-Bensaude. Car, de toute façon, le signalement est déjà une dérogation au secret médical (article 226-14 du Code pénal). « On ne partage pas un secret. En revanche, entre personnes qui prennent part à la protection de l'enfant, le fait de se communiquer uniquement ce qui

est nécessaire à son bien-être, c'est aider au traitement. »

C'est en partie pour remédier à ce type de dysfonctionnements que le ministre, Philippe Bas, propose d'ouvrir, au sein du conseil général, une « cellule de signalement » animée par l'Aide

sociale à l'enfance. Cette structure serait alors chargée de centraliser ces informations et permettrait des prises de décision collégiales.

Les fondements de notre système de protection de l'enfance sont donc « solides et justes », estime le ministre. Mais lui aussi admet ses failles : « Est-il normal que dans un pays où l'on dépense plus de 5 milliards d'euros pour la protection de l'enfance, seulement 4 % de ces sommes soient consacrées à la prévention ? » ● PAMELA MESSI



Rhône

La Maison des adolescents

Un lieu d'écoute et d'accompagnement



Vue du dispensaire général de Lyon, rue Sévigné (III^e arrondissement), où va être hébergée, dans un premier temps, la Maison des adolescents de la Mutualité française du Rhône.

Vers une spécialité à part entière ?

Notre pays a un faible pour la classification et, en médecine, un goût certain pour les spécialités. Va-t-on vers la naissance d'une nouvelle spécialité médicale, la médecine de l'adolescence, tant les questions de santé des 16-25 ans apparaissent à la fois spécifiques et complexes ? En tout cas, après le premier congrès national des maisons de l'adolescent, qui vient de se tenir au Havre (il y a une quinzaine de MDA en France, y compris celles encore à l'état de projet), il semble que cette idée chemine. Des spécialistes reconnaissent que, quel que soit leur mode d'exercice, les professionnels de santé de tous horizons sont fréquemment demandeurs. L'un des leaders de la pédopsychiatrie, le professeur Marcel Rufo, chef de service à la Maison de Soléon (hôpital Cochin, Paris), plaide même pour la création d'un diplôme d'études spécialisées complémentaires d'un ou deux ans.

Soigner et accompagner, en coordination avec les structures et les professionnels de santé spécialisés de l'agglomération lyonnaise, mais aussi devenir un lieu de formation et de recherche sur les problèmes de santé des adolescents : les missions assignées à la Maison des adolescents que la Mutualité va ouvrir au sein du dispensaire Sévigné, dans le III^e arrondissement, sont multiples.

La Maison des adolescents (MDA), dont le projet est en préparation depuis plusieurs mois sous la houlette de Christophe Porot, responsable du service Promotion de la santé à la Mutualité du Rhône, et du psychiatre Kostas Nassikas (clinique mutualiste), va bientôt ouvrir ses portes au sein du dispensaire Sévigné, 10, rue Sévigné dans le III^e arrondissement de Lyon.

Accueil, aiguillage

Les adolescents et les jeunes adultes ont-ils des besoins de santé à ce point spécifiques qu'il faille leur dédier une structure chargée de leur offrir une réponse thérapeutique immédiate ou de les orienter vers tel ou tel professionnel de santé en fonction des besoins ? La réponse semble

positive. « On sait qu'environ 10 % d'entre eux souffrent de troubles psychologiques, résume Christophe Porot. Or ces troubles sous-jacents peuvent entraîner des difficultés chroniques au niveau du sommeil, de l'alimentation, ou susciter des conduites violentes ou antisociales. » On sait aussi,

ajoute-t-il, que « la consommation de produits licites ou illicites – un adolescent sur deux déclare fumer, 10 à 20 % ont une consommation régulière d'alcool, 15 à 25 % fument régulièrement du cannabis, 5 % de l'héroïne, du LSD, de l'ecstasy... – est loin d'être marginale chez les 16-25 ans.

Formation et recherche

La MDA lyonnaise ne sera pas qu'un lieu de soins et d'orientation. Elle aspire à juste titre, dans un domaine où beaucoup reste à explorer et où les « lieux-ressources » sont rarissimes, à devenir un lieu de réflexion et de recherche, bref, un lieu de référence sur les questions multiples que soulève l'adolescence. Il existe chez les professionnels du médico-social de grands besoins en formation, notamment dans un champ cher à la Mutualité, celui de la prévention.



Sans oublier divers problèmes de santé plus connus et pouvant frapper leurs aînés, tels que la dépression, les troubles du comportement alimentaire (boulimie, anorexie) ou du métabolisme, ou encore les affections gynécologiques. »

Culture de l'adolescence

Un certain nombre de constats plaident aussi en faveur de l'ouverture de maisons spécialement dédiées à la santé de cette tranche d'âge. Ainsi, les enquêtes montrent que les ados tardent à recourir au système de soins, qu'ils ne vont chez le généraliste ou le psy qu'à reculons, beaucoup renonçant même à toute démarche de soins. Parallèlement, nombre de professionnels de santé, publics ou libéraux, n'ont qu'une approche très théorique des maux de l'adolescence. Dès lors, insistent Christophe Porot et Kostas Nassikas, « médecins, soignants et travailleurs sociaux sont rares à avoir une vraie culture de l'adolescence ». Parmi ses objectifs ambitieux, la MDA de Lyon espère donc contribuer à développer cette culture chez tous les intervenants médico-sociaux en lien avec elle, médecins prescripteurs, bien sûr, mais aussi médecins scolaires, professionnels de la PMI, du Planning familial, de la justice, etc. Bref, la MDA entend mettre progressivement sur pied un véritable « réseau de santé de l'adolescence » dans le Rhône. A l'arrière-plan, on l'aura compris, deux paris sont engagés.

Le premier: devenir très vite un « lieu-ressource » facile à fréquenter, aisé d'accès, gratuit pour tous, en tout cas dans un premier temps (pour l'aspect « droits sociaux », une assistante sociale sera présente au sein de la maison), l'objectif étant de répondre dans la souplesse à toute la palette des demandes somatiques et psychologiques des jeunes gens; et simultanément, en fonction des demandes exprimées, jouer le rôle de conseil d'orientation en proposant un parcours bien fléché. Le second pari de la MDA, à moyen terme, est d'apparaître au sein l'agglomération lyonnaise comme « le » lieu de référence stratégique pour la formation et la recherche sur l'adolescence (lire l'encadré en page VI).

A noter enfin que la MDA sera pilotée par une personne chargée notamment de la

Freiner la progression de l'obésité infantile

N'est-il pas trop tard pour freiner l'augmentation de l'obésité chez les tout-petits? L'association lyonnaise Repori, Réseau pour la prévention de l'obésité pédiatrique, veut le croire, quelle que vaille que vaille, grâce à un vaste réseau de professionnels de santé, de faire passer dans l'agglomération le message selon lequel une prévention la plus précoce possible est impérative. Médecins, psychologues, diététiciens, kinés, constatent que l'impact de l'obésité infantile, de plus en plus tôt, des campagnes de prévention incitant à la vigilance (alimentation, exercice physique, etc.) jouent probablement leur rôle à la marge, mais les professionnels sont unanimes à recommander un geste simple qu'il convient aux parents: la surveillance régulière chez le médecin - au moins une fois par an - du poids de l'enfant, puis de comparaison de cette donnée avec la courbe normale des 1000 premiers jours.

Repori (MDA) 73 50 00 00

coordination avec les professionnels de santé de l'agglomération, qu'une procédure d'évaluation de la structure est évidemment prévue et qu'un site Internet est en préparation pour améliorer la communication. ♦ G.C.



L'obésité chez l'adolescent S'adapter au sujet et mettre en confiance



En France, deux millions de sujets âgés de 0 à 18 ans souffrent d'obésité, soit 15 % de la population française. S'il est souvent question des conséquences physiologiques de l'obésité chez l'adolescent, il ne faut pas sous-estimer les conséquences psychologiques dues à cette pathologie. C'est pourquoi la prise en charge doit être globale et faire l'objet d'un projet thérapeutique adapté à chacun.

A lors que la région Midi-Pyrénées recense près de 10 000 enfants obèses, la Maison d'Enfants Diététique et Thermale de Capvern-les-Bains, dirigée par le Docteur Roggero, s'est spécialisée dans la prise en charge globale de l'obésité résistante chez l'adolescent âgé de 14 à 17 ans.

Comment assurer une prise en charge du sujet dans sa globalité? Comment s'adapter à chaque cas particulier et mettre en confiance l'adolescent afin de l'engager dans un processus d'amai-grissement durable?

La maison d'enfants diététique et thermale de Capvern-les-Bains est située dans une charmante station thermale des Hautes-Pyrénées, à 400 mètres d'altitude. Dans un cadre naturel exceptionnel, l'établissement est établi dans les murs d'un ancien hôtel "Le Beau Séjour", réaménagé par l'association "Soleil et Bigorre" pour donner vie à la maison d'enfants dont les 24 salariés accueillent en permanence 45 jeunes patients.

La structure principale est composée de trois niveaux : trois lieux de vie selon l'âge, un par étage, avec pour chacun trois éducateurs, chacun de ces professionnels étant "pilote de projet" pour 3 à 6 jeunes patients.

Un séjour adapté à la pathologie de l'adolescent

Le recours à la maison d'enfants diététique et thermale est majoritairement conseillé par le médecin traitant de l'adolescent lorsque la prise en charge ambulatoire s'avère insuffisante et que la situation paraît nécessiter une conduite thé-



© Photo Alain Buzza

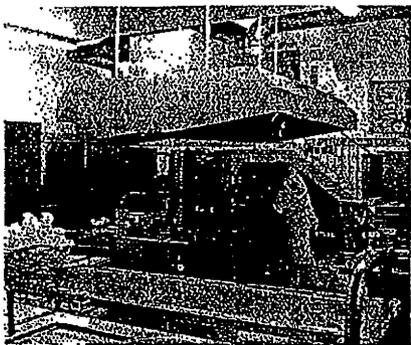
rapeutique globale approfondie. Il est fondamental dans le traitement de l'obésité de s'assurer de la volonté de l'adolescent, évaluée lors de la visite de préadmission et de mobiliser les capacités parentales. La motivation du sujet face au changement sera également mesurée lors des séjours proposés.

Le type de séjour est évalué par le médecin traitant qui indique celui qu'il juge le plus adapté à la pathologie de l'adolescent. Durant toute la durée du séjour, aura lieu un échange d'informations en continu entre le médecin traitant et l'équipe pluridisciplinaire. L'établissement et le médecin traitant enrichissent ainsi leur réseau de soins actuel et futur.

Différents types de prises en charge

La maison d'enfants propose différents types de prises en charge adaptés au parcours de l'adolescent, à son lieu de résidence, à son âge, son sexe, sa pathologie, aux objectifs thérapeutiques prédéfinis et à son projet personnel :

- le Séjour de Formation Intensive et d'Ori-entation (S.F.I.O.) se déroule sur 15 jours pendant les vacances scolaires. Il permet de mesurer la motivation du patient par rapport au dispositif thérapeutique et socio-éducatif ainsi que ses facultés à s'adapter à l'internat. Ce séjour permet également à l'adolescent de mettre sa motivation à l'épreuve de la réalité des offres thérapeutiques qui lui sont proposées
- le Séjour de Formation Intensive et de Réorientation (SFIR), également d'une durée de 15 jours, est renouvelable plusieurs fois. Il permet de réajuster le relais qui a été pris par la famille et de réactualiser le projet thérapeutique d'une prise en charge par des courts séjours
- un Séjour d'évaluation d'un mois pendant les vacances scolaires de juillet ou d'août est toujours réalisé en préalable à un éventuel séjour de l'année scolaire
- un séjour curatif de 10 mois pendant une année scolaire. Ce séjour est proposé pour les jeunes patients considérés comme prêts pour le traitement de l'obésité en internat. La scolarité est obligatoire et elle est assurée au collège et lycée de l'Institution Notre-Dame de Garaison. A la fin du séjour, l'équipe pluridisciplinaire propose



© Photo Soleil et Bigorre

le travail à engager ou la nouvelle orientation à donner.

Lors de ces séjours, la prise en charge de l'adolescent se fait selon le protocole précis d'un contrat médico-psycho-éducatif. Le but du traitement ne peut se réduire à la perte de poids : le projet thérapeutique doit à tout prix intégrer des objectifs psychologiques et sociaux individualisés.

Un suivi pluridisciplinaire pour chaque adolescent

La maison d'enfants propose donc pour chaque adolescent accueilli un suivi pluridisciplinaire dans le cadre d'un projet thérapeutique individuel qui sera établi en commun avec le jeune patient selon ses besoins médicaux, socio-éducatifs et psychologiques. L'adolescent doit, de son côté, présenter par écrit un projet personnel dont les évolutions seront discutées au fur et à mesure du séjour.

La coordination du projet individuel et du projet personnel du patient sera assurée par le Docteur Roggero, médecin de l'établissement, en ce qui concerne les champs médicaux, diététiques, physiques, sportifs, socio-éducatifs, psychologiques et scolaires. Le pilotage de la relation dynamique entre ces deux projets sera du ressort de l'éducateur "pilote de projet" qui parti-

cipe à l'organisation et à l'animation du quotidien, soutient le travail des jeunes patients et les aide à atteindre les objectifs fixés pour le séjour. Il favorise également l'insertion sociale et scolaire de l'adolescent, assure le lien avec la famille, l'institution scolaire et toute l'équipe de l'établissement.

L'importance du rôle des parents

L'éducation étant primordiale dans le phénomène de l'obésité, le rôle des parents est très important dans la continuité du projet thérapeutique de l'adolescent. La famille est donc reçue en début de séjour et visite les lieux lors des rencontres de préadmission ou d'entrée. Cette rencontre est obligatoire. Un bilan peut se faire également à tout moment à la demande de la famille ou de l'équipe lorsque la situation le justifie.

En pratique, le traitement de l'obésité passe par la recherche d'un équilibre sur les plans alimentaires, physiques et sportifs ainsi que sur toutes autres variables pertinentes. Le jeune patient découvre la réalité du lien social et les effets d'une activité alimentaire équilibrée adaptée aux besoins de son corps. Les consultations avec la diététicienne sont périodiques et à la demande tout comme pour les autres professionnels intervenants. Les actions pédagogiques permettront aux jeunes patients de savoir cuisiner, apprentissage indispensable pour la gestion quotidienne du poids et pour faire face aux aléas de la vie.

Des prises en charge complémentaires

Les prises en charge diététique, physique et sportive sont complémentaires les unes des autres. Une activité physique régulière est indispensable dans le délicat travail d'équilibrage de la

balance énergétique. L'éducation physique et sportive est donc obligatoire pour le jeune patient dans le cadre du traitement de l'obésité proposé par la maison d'enfants diététique et thermale. Les différentes activités sportives sont approfondies après évaluation du profil de chacun : capacités, relationnel envers les autres et par rapport à l'activité, apprentissage et motivation. Le but de l'établissement est d'amener chaque jeune patient à pratiquer volontairement et régulièrement une activité physique et/ou sportive. Il s'agit de faire connaître aux jeunes le plaisir de faire du sport mais aussi de restaurer l'estime de soi et d'améliorer l'image du corps pour acquérir un certain mieux-être social.

La maison d'enfants propose également de multiples activités socio-culturelles visant à favoriser l'expression des potentiels de chacun.

La mise en tension du projet personnel de l'adolescent et du projet individuel de la maison d'enfants est en soi la pratique d'une méthodologie de résolution de problèmes. C'est le management d'un plan d'action par objectifs négociés qui fait émerger chez le jeune patient ses ressources propres. Il bâtit intérieurement un sentiment de confiance provenant du vécu de l'expérience et du fait qu'il ait réussi lui-même à surmonter les obstacles. Avoir réalisé ce travail sur soi au sein de sa classe d'âges, en interaction avec les professionnels et sa famille, lui a permis d'acquérir des apprentissages sociaux fondamentaux et de tisser des liens solitaires durables avec ses pairs.

Ce ne sont ni les messages d'encouragement des anciens pensionnaires ni les lettres reçues des années après qui démentiront l'efficacité résultant de l'esprit de convivialité, du sérieux et de la détermination de l'équipe pluridisciplinaire dans la prise en charge de ces adolescents. Pour preuve de son implication, la maison d'enfants diététique et thermale a d'ailleurs accueilli le 20 mai dernier la vingtaine de maisons d'enfants existantes spécialisées dans l'obésité infantile afin de débattre de la prise en charge de cette pathologie dans le cadre d'ateliers thématiques réunissant 70 professionnels de toutes disciplines. ■

Docteur Jean-Louis Roggero,
Médecin-directeur de la Maison d'Enfants
Agnès Vallet,
Chargée de mission FEHAP

Maison d'Enfants "Soleil et Bigorre"
65130 Capvern-Bains
Tél. : 05 62 40 90 90 - Fax : 05 62 40 90 80



© Photo Soleil et Bigorre

Répondre au mal-être des jeunes

Les troubles rencontrés par les adolescents sont à prendre au sérieux: en dix ans ils ont augmenté de près de 70%. Pour répondre à ce mal-être, des structures fonctionnant en réseau apportent des réponses innovantes aux jeunes en désarroi mais aussi aux équipes qui les soignent.



transformation physique irréversible, évolution psychologique souvent paradoxale et changements sociaux plus ou moins progressifs, l'adolescence correspond à une étape charnière de l'existence. Selon une récente enquête Ipsos Santé⁽¹⁾, un adolescent sur deux déclare avoir déjà rencontré un problème de nature importante. En majorité d'ordre familial, des difficultés peuvent aussi apparaître au niveau scolaire, sentimental, psychologique ou addictif. Point plus inquiétant: l'enquête révèle une augmentation impressionnante des troubles psychiatriques chez les adolescents. Entre 1991 et 2001, le nombre d'enfants suivis en psychiatrie infanto-

juvénile est passé de 16 à 28 pour 1 000, soit une augmentation de près de 70%. Pourquoi un tel boum? Une société à la fois plus anxieuse et plus démonstrative, des adultes très exigeants envers les plus jeunes, des ados qui ne trouvent pas toujours les réponses à leurs attentes... Les explications découlent en grande partie de notre mode de vie. Si la plupart des jeunes rencontrant des difficultés se tournent vers leur entourage pour s'en sortir, pour les situations les plus graves, une aide extérieure s'avère nécessaire. Les structures d'accompagnement jouent donc un rôle indispensable dans la prise en charge du malaise des adolescents. L'Institut Mutualiste Montsouris

(IMM), fut l'un des précurseurs en la matière. Depuis les années 70, un département de psychiatrie de l'adolescent et du jeune adulte, dirigé par le Professeur Philippe Jeammet, s'adresse aux jeunes présentant des problèmes psychologiques ou des troubles avérés (voir interview p. 27). Une équipe composée de psychiatres, psychologues et assistantes sociales, propose des consultations d'évaluation et d'orientation ainsi que des suivis thérapeutiques ambulatoires. Une consultation sans rendez-vous, une fois par semaine, permet également

1. Enquête réalisée pour la fondation Wyeth du 16 au 23 mars 2005, auprès de jeunes âgés de 13 à 18 ans. Consultable sur www.ipsos.fr/CanalIpsos/articles/1587.asp



L'adolescence est un moment charnière de la vie. Confrontés à des bouleversements de tous ordres, garçons et filles expriment leurs souffrances à travers des symptômes de plus en plus visibles.

d'accueillir des jeunes pour les orienter et répondre à leurs besoins. C'est, en France, le service le plus important dédié à l'adolescence. Dans des locaux modernes, accueillants et ouverts, plus de 2 000 jeunes de 13 à 20 ans viennent consulter chaque année. Le département psychiatrique compte 38 lits d'hospitalisation (dont 8 d'urgence) et 30 places en hôpital de jour. Des spécialités se sont progressivement développées dans les domaines des troubles du comportement alimentaire, de la dépression et des tentatives de suicide.

Thérapie bifocale

Cette unité a servi de modèle aux nombreuses structures qui ont vu le jour par la suite. En effet, la qualité de l'accueil, les compétences dans l'évaluation et les capacités à suivre les adolescents sur le long terme sont les atouts majeurs de ce service. Les suivis associent, selon les situations, différents types d'interventions auprès du patient et de sa famille. L'équipe utilise une technique appelée thérapie bifocale : un médecin référent accompagne l'enfant dans son projet thérapeutique. Il peut s'appuyer sur d'autres thérapeutes, mais reste le garant de la continuité du projet. Cet aspect éducatif fondamental

permet une continuité dans le traitement, mais aussi de suivre davantage d'adolescents, en aménageant leur traitement selon leur évolution et en s'intéressant à ce qu'ils deviennent dans la durée.

Le département psychiatrique fonctionne en réseau. Il est composé de plusieurs unités parmi lesquelles le DERPAD. Créé en 1996, le Dispositif expert régional pour adolescents en difficulté associe l'IMM,

la MFP, la Direction générale de la Protection Judiciaire de la Jeunesse, la Direction régionale de l'Administration pénitentiaire et l'Agence régionale de l'hospitalisation. A l'interface santé-justice, il a pour mission d'apporter de nouveaux outils aux équipes sanitaires, éducatives, sociales et pédagogiques de l'Île-de-France confrontées à des situations particulièrement difficiles. « L'idée de départ était de faire évoluer l'offre de service en articulant le soin et l'éducatif. Il existait déjà beaucoup d'institutions travaillant avec les jeunes, mais rien n'était fait en direction de ces professionnels », explique le docteur Jean-Michel Hervieux, directeur médical du DERPAD. Cette unité n'est donc pas directement en contact avec les adolescents, mais donne des outils à ceux qui les prennent en charge pour résoudre les difficultés rencontrées.

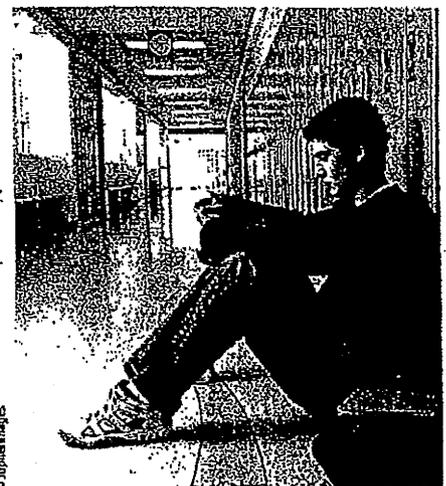
Accompagner les soignants

La consultation est la colonne vertébrale du dispositif. « Quand un psychologue, un éducateur ou une institution se retrouve dans une impasse face à un jeune, nous le rencontrons pour mettre à plat la situation qui pose problème, pour comprendre où se situe le blocage et chercher les moyens de le lever », souligne la directrice éducatrice du DERPAD, Christine

Chinosi, avant de préciser que « cette consultation est gratuite, anonyme et confidentielle ». Les professionnels sont toujours reçus à deux : par un membre de l'équipe sanitaire et un membre de l'équipe éducative. « Cette consultation est l'occasion de prendre de la distance car ces professionnels sont souvent très impliqués et les situations – placement, incestes, maltraitance – difficiles » ajoute Jean-Michel Hervieux.

Le binôme apporte ainsi un regard neuf. Le DERPAD est un lieu de parole libre où aucun rapport hiérarchique ne vient entraver la discussion. Pour Christine Chinosi, « une consultation est réussie quand il y a eu suffisamment d'alchimie, quand le professionnel repart motivé avec des pistes de travail ». Depuis 10 ans, ce dispositif, jusqu'alors expérimental, a fait ses preuves : dans 75 % des cas, la situation du jeune s'en trouve améliorée. Pour le pérenniser, un groupement d'intérêt public s'est constitué, associant les partenaires initiaux. « Le soutien sans faille de la MFP et de l'IMM nous a été précieux pour obtenir un cadre juridique jusqu'ici informel », conclut le docteur Hervieux. En devenant une entité juridique autonome, le DERPAD acquiert à la fois une reconnaissance de son travail et une souplesse dans sa manière de répondre aux professionnels.

Claire Chognot



Les troubles psychiatriques des adolescents ont progressé de façon inquiétante durant les dix dernières années.

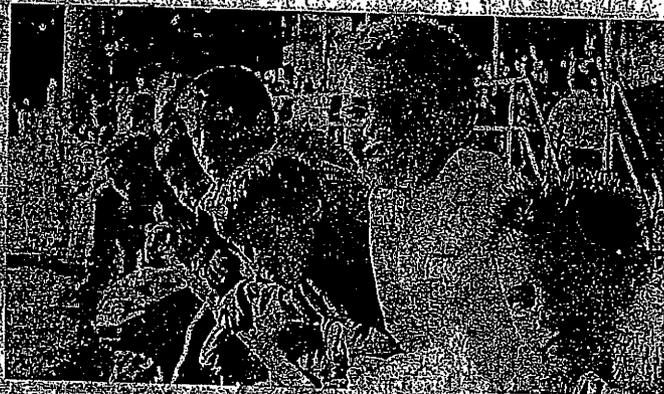
OF 26.10.06

Pays de Vie et Pays de Monts

600 collégiens contre les leucodystrophies

Mardi matin, les élèves de Garcie Ferrande ont participé au deuxième cross de l'établissement. Pour la bonne cause.

Quand on est bien mais court pour une bonne cause, c'est mieux. Mardi matin, 600 collégiens de Garcie Ferrande ont participé au cross de leur établissement, selon l'association "Mars Basket Sports" à Madrid. Ce slogan est celui de la "Sociation" et se traduit par "utilité publique" ou "lutte contre les leucodystrophies". Un groupe de maladies génétiques qui affectent le système nerveux central et peuvent entraîner la paralysie, l'endocardite, la cécité, la surdité, l'amaurose, etc. L'association "Mars Basket Sports" a été créée par des enseignants et des parents d'élèves. Avec les autres enseignants, on se dit qu'il pourrait être intéressant de s'engager avec les élèves pour cette cause, explique Anne Allegret, coordinatrice des professeurs d'EPS. Quand on voit des élèves qui n'ont pas envie de faire du sport, on leur dit "promenez-vous". Alors, après avoir remis le parcours en état suite aux coups de vents violents de la veille, les collégiens ont pris part à cinq courses distinctes, par tranches



Afin de mettre en place ce cross, les élèves ont fait appel à des parents pour récolter des dons. Ils seront reversés à la lutte contre les leucodystrophies. L'association "Mars Basket Sports" a été créée par des enseignants et des parents d'élèves. Avec les autres enseignants, on se dit qu'il pourrait être intéressant de s'engager avec les élèves pour cette cause, explique Anne Allegret, coordinatrice des professeurs d'EPS. Quand on voit des élèves qui n'ont pas envie de faire du sport, on leur dit "promenez-vous". Alors, après avoir remis le parcours en état suite aux coups de vents violents de la veille, les collégiens ont pris part à cinq courses distinctes, par tranches d'âge, à travers des circuits allant de 2000 à 6000 mètres. C'est une sorte de conclusion du cycle d'endurance, explique Anne Allegret. Nous commençons souvent l'année scolaire par l'endurance. C'est aussi une

Société III Jeunes

L'EXPRESSION DU MAL-ÊTRE DES ADO...

FILLES



GARÇONS



Lien social n° 772
03.11.2005

Faire de la prévention, mais dans quel but ?

Dr Bernard LELU

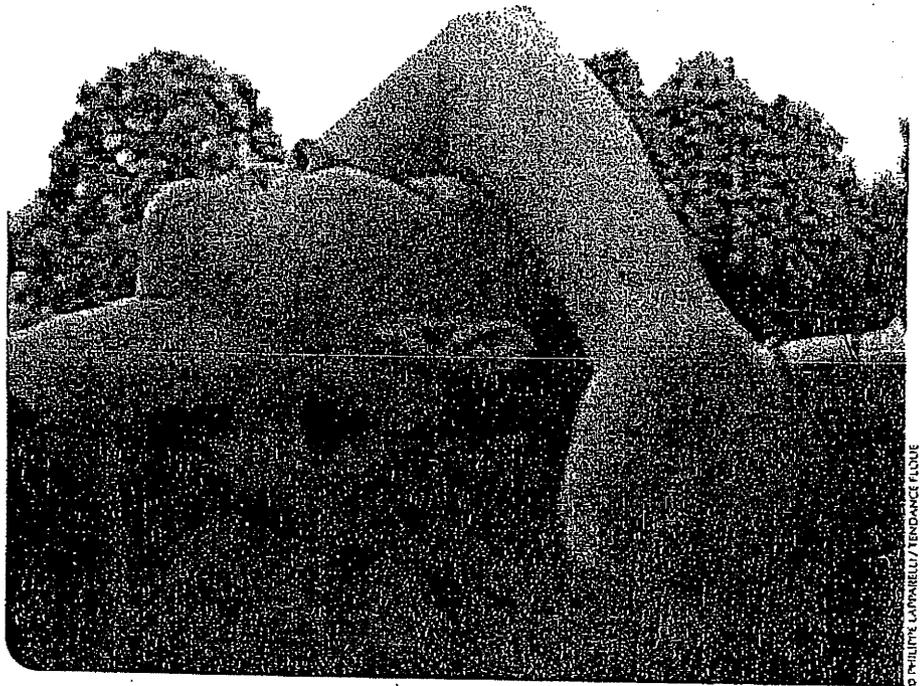
Médecin directeur des Universités

Cette question semble *a priori* évidente, pourtant la finalité de la réponse me semble plus complexe.

Avant de commencer à réfléchir sur les problématiques de santé, si le but recherché en ce qui concerne le curatif amène rapidement à un consensus (trouver la meilleure thérapeutique pour un résultat visant la guérison), l'objectif final de la prévention n'a pas forcément la même réponse unifiée.

La solution est-elle culturelle, financière, idéologique ? Permet-elle à chacun de construire sa vie dans un épanouissement physique et psychique tout en limitant les facteurs de risque ?

Faut-il « normater » un modèle ou un concept de vie qui permettrait de prolonger l'espérance de vie ? Mais alors dans quelles conditions ? Ces questions sont essentielles dans l'approche du concept de prévention ; et la normalité se pose souvent non pas par rapport à des règles de fonctionnement physiologique ou médicale mais par rapport à une « norme sociale » ou philosophique. L'apprentissage du respect du corps, la compréhension de ses fonctions et la recherche d'un « bien-être », qui sont autant de clés d'une construction harmonieuse, doivent être au centre de l'éducation à la santé des enfants. **Apprendre la notion du plaisir** me paraît aussi fondamentale car elle ne se construit pas sur l'interdit mais sur la recherche d'un équilibre. Le plaisir au sens épicurien est de cultiver le bien-être sans excès en limitant les risques. Nous voyons que le concept préventif devrait être pris au sens large tel que le définit l'OMS englobant de nombreux facteurs. À travers ces quelques lignes, j'ai voulu soulevé des réflexions que chaque acteur devrait se poser avant toute démarche ; réflexions d'autant plus importantes lorsque que les acteurs sont issus de formations différentes brassant ainsi une richesse de points de vue et d'expériences permettant d'approfondir le but recherché.



© PHILIPPE LAPINELLI / BONDANCE FACILE

Définition de la promotion de la santé

« La promotion de la santé a pour but de donner aux individus davantage de maîtrise de leur propre santé et davantage de moyens de l'améliorer. Pour parvenir à un état de complet bien-être physique, mental et social, l'individu, ou la groupe, doit pouvoir identifier et réaliser ses ambitions, satisfaire ses besoins, et évoluer dans son milieu ou s'y adapter. La santé est donc perçue comme une ressource de la vie quotidienne et non comme le but de la vie ; c'est un concept positif mettant l'accent sur les ressources sociales et personnelles, et sur les capacités physiques. La promotion de la santé ne relève donc pas seulement du secteur de la santé : elle ne se borne pas seulement à préconiser l'adoption de modes de vie qui favorisent la bonne santé ; son ambition est le bien-être complet de l'individu. »

*Extrait de la Charte d'Ottawa,
le 21 novembre 1986*

Définition de la santé

« La santé est un état de complet bien-être physique, mental et social, et ne consiste pas seulement en une absence de maladie ou d'infirmité. »

*Extrait de Constitution de l'Organisation mondiale
de la santé adoptée le 22 juillet 1946
et entrée en vigueur le 7 avril 1948*

ADOSEN n.°148 - Juin 2005