zelig.rc2

...activistes, cyberfeministes, syndicalistes, intellos pr´caires, nerds, hackers, gender changer, cyborgs, mutant(e)s, newbies, travailleurs immatériels, codeurs et codeuses, hacktivistes, militant(e)s, technojunkies, hybrides, bad grrrls... **Paris 9-15 décembre 2002**

L'information veut être libre

Qu'est-ce que la **zelig.rc2** ? Du 9 au 15 décembre prochain, une semaine d'ateliers, démos, rencontres, débats, autour des réseaux, de la communication, du logiciel libre et de la résistance électronique. Une semaine où l'on parlera de technique, de politique, de désirs, de créations, de mouvements... Après la rencontre européenne de décembre 2000 (zeligConf), et la rencontre hexagonale de février 2001 (no-zelig), nous souhaitons de nouveau ouvrir un laboratoire temporaire de communication, un espace-temps de circulation des savoirs et des savoirs faire, une zone autonome où puissent converger et se combiner les cultures de l'activisme et celle du *hack*, les pratiques de contre-information et le génie productif du logiciel libre, la créativité des acteurs des mouvements sociaux et celle des diverses communautés des réseaux. Cette fois encore nous voulons donc faire le pari du mixage des expériences, de l'hybridation des identités, de la transversalité des réflexions et des pratiques. Nous voulons faire le pari de la coopération productive entre les réalités multiples de la contestation et de l'innovation sociales qui agissent dans les replis du réel.

La **zelig.rc2** s'articulera autour d'un ensemble de thèmes, qui donneront lieu tant à des ateliers pratiques et présentations, que des rencontres, conférences et débats. Une diversité de formes qui, nous l'espérons, permettra de combiner approche technique et approche politique de l'ensemble des questions abordées.

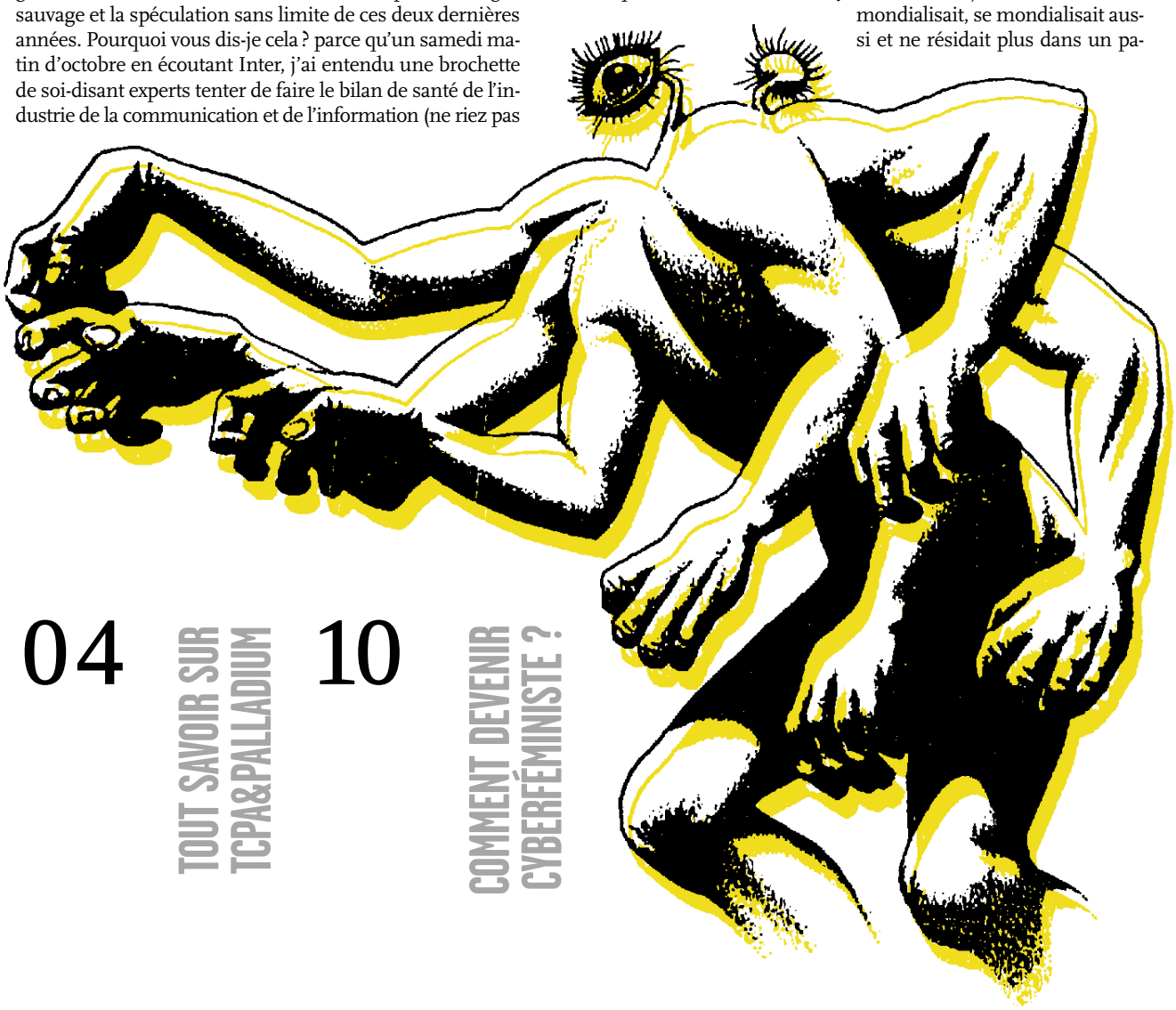
- Résistance électronique : protection des données personnelles, confidentialité des échanges via l'Internet, sécurisation d'ordinateurs, désobéissances à la surveillance généralisée, charte du « travailleur numérique ».
- Cyberfeminism is an attitude : genre et technologie, identité et machine. Théories et pratiques de ces badgirls qui aiment les machines et jouent avec l'identité
- Communication alternative : les outils (publication sur le web, mailing lists), les expériences (sindominio, collectifs. net, samizdat. net, Indymedia, etc.), la confrontation au pouvoir médiatique, la coopération au niveau européen.

Entre les mailles de ces thématiques, seront aussi ouverts divers chantiers. En particulier : logiciel libre pour les enfants et l'éducation, ressources pour les réseaux associatifs (*firewall*, démocratie interne), communication sans-fils (*WiFi*), outils logiciels pour la contestation électronique (*Reamweaver*), etc.
Enfin, la zelig.rc2 sera l'occasion de présenter un certains nombre d'initiatives et de projets : no-log (services de connexions non-loguées), l'Autre net (hébergement alternatif), AlternC (kit logiciel pour l'hébergement de sites web), Plug'n'Politix (initiative), Glastnost (Intranet pour association), Libre entreprise, Fédération informatique et liberté, hacklabs (Italie, Espagne)...
Avec ce melting pot de prétextes pour se voir et de s'émouvoir, nous entendons rappeler ce bon vieux principe hacker : l'information veut être libre. Elle ne le doit pas, sur le mode d'une injonction impuissante, elle le veut, parce que l'enjeu politique est celui de notre liberté de circuler, de penser, de coder, de parler, d'aimer, de créer, d'innover. L'information veut être libre, parce qu'elle ne peut être soumise ni aux diktats marchands, ni aux injonctions policières.

Paris le 3 octobre 2002
zelig.rc2

Une cheville ronde dans un trou carré !

S'il est une obsession de ce troisième millénaire que l'on nous promet de nous faire tant aimer, largement amplifiée par le 9-11, c'est bien celle de l'identification des personnes. On part d'un algorithme simple « if/then » : « si » certains sont terrroristes ou criminels ou simplement délinquants, « alors » nous le sommes potentiellement tous. Il convient donc d'anticiper sur l'acte. Ce qui pour nos sociétés dites démocratiques signifie identifier chaque suspect, chaque perturbateur réel ou virtuel, chaque contestataire avant qu'il n'ait commis la chose. Et pour ce faire, elles mettent en place une véritable nasse technologique, un filet anti-terroriste-criminalité-délinquance, un réseau sécuritaire planétaire qui aura – ce n'est pas négligeable à l'heure actuelle – l'avantage de relancer une économie mise à mal par la dérégulation sauvage et la spéculation sans limite de ces deux dernières années. Pourquoi vous dis-je cela ? parce qu'un samedi matin d'octobre en écoutant Inter, j'ai entendu une brochette de soi-disant experts tenter de faire le bilan de santé de l'industrie de la communication et de l'information (ne riez pas c'est tout ce qu'il y a de sérieux). Parce que la veille, au treize-quatorze sur la même radio, l'animateur de l'émission Fabrice Drouelle évoquait « le problème croissant des infractions routières au permis de conduire », forme nouvelle de ce que l'on qualifie de « nouvelle criminalité » puisqu'aujourd'hui tout est peu ou prou criminel. Selon les statistiques – connues pour être, comme les experts, un outil politique et fabricateur d'opinion au service du pouvoir – de plus en plus de chauffards conduiraient sans permis. Partant de là, un expert, M. Christophe Naudin, chercheur au département de Recherche sur les menaces criminelles contemporaines (DRMCC) interrogé par le journaliste sur l'éventualité d'un permis de conduire infalsifiable, déclara benoitement que les papiers – l'identité anthropométrique – étaient obsolètes. Que l'identité aujourd'hui où tout se mondialisait, se mondialisait aussi et ne résidait plus dans un patronyme culturellement référencé, donc dans un document matériel – falsifiable ou non – mais dans le corps. Que nous étions notre corps et vice-versa et qu'en se donnant la possibilité technique de scanner ce corps par tous les bouts, on pourrait, on saurait identifier à tout coup. Le corps est notre support identitaire, et la biométrie le remède miracle pour la planète. L'industrie des TI (technologies de l'information) peut se lécher les babines, le gisement est énorme : six milliards d'individus !



Qui était donc ce si catégorique expert ? *Google – searching, searching, searching*... et le voilà, lui aussi identifié : Christophe Naudin, auteur d'un mémoire pour son diplôme universitaire en 2000 (expérience professionnelle bien courte pour un expert au DRMCC) sur *Les fausses identités : une criminalité aux conséquences volontairement ignorées* (2), dont l'un des derniers chapitres « Prospective » contient un sous-chapitre intitulé « L'identité absolue » dont la lecture est édifiante. Quant au DRMCC (3), il s'agit d'une unité de recherche de la Sorbonne, pilotée par Xavier Raufer (5), connu dans les milieux informés comme expert es sécurité, qui se donne pour mission de : « accroître la connaissance des phénomènes criminels contemporains, nationaux ou transnationaux, qui menacent nos sociétés, dans toutes leurs dimensions, juridiques, criminologiques, sociales, culturelles, financières... » parmi lesquels phénomènes on trouve, outre le terrorisme et le crime organisé, « les guérillas dénaturées » (sic), les « micro-cultures violentes » et l'« écoterrorisme/bioterrorisme ». Je vous laisse apprécier.
Le DRMCC se propose de « conceptualiser les éléments caractéristiques de la menace » et de faire « des propositions concrètes en vue de créer ou de renforcer les moyens juridiques de lutte contre ces phénomènes criminels ». Autrement dit se place comme pépinière d'experts, diplomés et savants auprès des cabinets, collectivités locales et médias concernés par l'insécurité. Ces experts que Pierre Rimbert (4) nomme « les managers de l'insécurité » : des « chercheurs [qui s'affirment] dépositaires d'un savoir juridique et statistique – [voire des] gardiens de l'ordre scientifique ». On leur doit les nouveaux vocables « zone de non-droit », « violences urbaines » et autres

« incivilités » qui émaillent tout discours sécuritaire de droite comme de gauche. On leur doit aussi des statistiques toujours plus explosives qui font monter la pression et que Rimbert qualifie de « construction comptable de l'insécurité ». Fort de ces cautions scientifiques et « apolitiques », leur discours « se donne pour incontestable [...], contre le tout répressif » voire même parfois « contestataire ». Xavier Raufer, directeur des Etudes et recherches-Séminaires du DRMCC et son accolyte Alain Bauer (6) sont parmi les plus connus de ces experts parisiens et vendent moultes conférences, prestations et expertises.

Mais revenons aux affirmations de notre expert du treize-quatorze, M. Naudin : au panier donc les CI, les permis, les passeports et autres cartes de séjour, cartons magnétiques et badges électroniques. Les garants de la sécurité, routière ou autre, disposent ou disposeront incessament sous peu d'un arsenal de systèmes introspectifs capables de dire si celui ou celle qui prétend être vous, l'est effectivement. Empreintes digitales, vocales, génétiques, forme de la main, de l'iris, du visage ou de l'oreille, tout est, paraît-il, unique à chacun(e) et reconnaissable, dès lors qu'il est déjà connu et archivé quelque part. La condition n'est pas anodine puisqu'elle induit que tous les citoyen(ne)s, ou disons tous les citoyen(ne)s suspects, soient fichés. Une fois tout le monde, pardon tous les suspects fichés, il n'est plus besoin que de systèmes de reconnaissance temps réel (plutôt onéreux) capables de scanner chaque fragment d'individu et de le comparer aux millions d'autres entreposés au préalable dans des bases de données. Le marché est global et n'attend que les spéculateurs pour devenir porteur. Analyse d'ADN, reconnaissance faciale, détection d'expression et de comportement, scanning immédiat des traces corporelles, de la forme de tel ou tel organe ou terminaison, sont autant de moyens incontournables et incontestables, disait notre expert, d'identifier ou d'authentifier.

Une minute, si vous permettez, pour tenter de saisir la différence entre ces deux termes. Authentifier c'est pouvoir dire avec certitude que la créature qui dit s'appeler A est bien la même que la créature A déjà « connue des services », autrement dit répertoriée dans la base. Identifier c'est pouvoir dire avec certitude que la créature X qui ne peut ou ne veut dire son nom est « connue des services » sous le nom de A ou B ou C. Exemple simple et juste un brin extrapolé. Je dis être journaliste depuis des années, mais je suis en réalité chomeuse depuis 5 ans, faisant des chantiers au noir. Sarkosy ayant décidé qu'un fichier des empreintes annales de tous les SDFs, RMistes et chomeurs de longue durée devaient être mis en place, je suis démasquée au premier contrôle routier. Seule solution abandonner ma voiture sur la route au premier appel de phare signalant un contrôle, mais las ! mes traces ADN sur le talus leur permettront de me retrouver sous quelques heures. Ou donner ma voiture et circuler habillée comme la femme invisible. Vous rigolez mais j'ai une amie qui a fait ça... donner sa voiture pour éviter ce genre de tracasseries.

Trève de plaisanteries, le raisonnement de cet expert, son hypothèse savante d'une identité absolue et infalsifiable sont atterants. D'autant plus qu'elle induit l'existence d'une police omniprésente et omni-connaissante, toujours prête à se glisser dans vos pensées pour dire si elles sont « correctes » ou non. Un scénario tout droit sorti des plus angoissants romans de SF. Aldous Huxley ne parlait-il pas dans sa préface à la réédition du *Meilleur des Mondes* en 1946 d'une « science complètement évoluée des différences humaines, permettant aux directeurs gouvernementaux d'assigner à tout individu donné sa place dans la société. (Les chevilles rondes dans des trous carrés ont tendance à avoir des idées dangereuses sur le système social et à contaminer les autres de leur mécontentement) ». Laquelle science associée à quelques autres conditions – « primo, une technique de conditionnement dans l'enfance [...] et à l'aide de drogues type scopolamine », secondo « un succédanné de l'alcool à la fois nocif et dispensateur de plaisir » pour fuir la réalité, tertio, « un système d'eugénique à toute épreuve pour standardiser le produit humain et faciliter la tâche des directeurs ». – permettrait de faire « aimer aux gens leur servitude » assurant ainsi la stabilité de l'Etat totipotent.

En serions nous déjà là ? L'identité au sens de la singularité de chacun(e) serait sur le point de disparaître. Gommée, éradiquée proprement. Chacun(e) devrait ressembler à l'autre, être sa copie, dérivée du même modèle génétique, physique ou mental. Ce qui attesterait alors de nous, de notre identité anthropométrique ne serait plus une photo ou un numéro sur une carte, mais un corpus de données, un data-corps, entreposé à jamais (si tant est que les machines et leurs mémoires soient immortelles) dans les mémoires du réseau, et identifiable par chacun de ses fragments. Un ensemble de *datas* prélevées sur chacun(e), éventuellement avant même la naissance, et stockées pour consultation ultérieure. Fragments de *je* et de *nous*, recompilés en temps réel à chaque contrôle. A cette cartographie charnelle intime viendraient s'ajouter au fil de la vie d'autres données complémentaires : où nous habitons, ce que nous mangons, ce que nous lisons, nos déplacements, lieux de vacances préférés, activités professionnelles et de loisirs, nos opinions politiques et religieuses, nos orientations sexuelles, et biensûr toutes entorses aux lois et règlements, toute déviation, toute différence et singularité ayant résisté à l'élagage. Cette incarnation informationnelle permettant de tirer notre portrait en toute occasion, de dessiner notre profil et de nous attribuer une note sur l'échelle de la suspiscion. Ou encore de nous vendre des produits inutiles mais « sur mesure ». Tout cela pour le plus grand bonheur d'une population de plus en plus inapte à se défendre et qui demande donc qu'« on » la protège. Ce qu'avait entrevu Huxley, une réalité imminente ? Subrepticement, sans que « les gens » s'en aperçoivent vraiment, et malgré les alertes lancées par les défenseurs des libertés ? Nous avons la science sécuritaire, nous avons le rêve et l'oubli distillés via l'hallucination consensuelle des médias et du réseau, et maintenant nous rêvons de prédétermination génétique. Méthode chère à Aldous, la « décantation des embryons » semble aujourd'hui à portée d'éprouvette. Les clones et autres tripatouillages hi-tech font régulièrement la une des médias qui agitent le pire sans trop s'engager. La modulation par conditionnement physique ou mental n'est pas si loin. Oh ! juste pour éradiquer les méchantes maladies. Et on va aimer ça. Et ça aussi ça va rapporter gros.

En 2002, la réponse à l'insécurité, c'est l'authentification et l'identification, la mise en fiches de la population, pardon des suspects, de tous les pays du monde. On parle de réduire chaque être humain à un numéro unique utilisé aussi bien pour la Sécu, les impots, le téléphone et l'internet. On parle aussi de plus en plus de dématérialiser cette preuve unique, ou plutot de la nano-turiser à l'échelle de l'atome et de l'implanter directement dans la chair. Marque indélébile, tatouée dans la matière qui rappelle les plus sordides épisodes de notre histoire. Il est question de faire de notre identité, à la fois endogène et exogène, modifiable dans une large mesure, une identité uniquement endogène et infalsifiable, intégrée au corps d'un coup d'agrafeuse technologique. *Schpoumfff !* La puce est presque dans votre avant-bras ou dans le lobe de votre oreille, design et efficacité garantis. Il n'est plus besoin que de vous scanner comme une vulgaire marchandise pour savoir qui vous êtes, où vous êtes et pourquoi vous y êtes. Dans un périmètre raisonnable il s'entend, mais sorti de ce périmètre, vous entrez de toute façon dans le suivant, et le suivant et le suivant.

Contrairement aux propos de notre expert, je pense que la sécurité n'est *pas* dans l'identification systématique, qu'une société qui surveille tous ses citoyen(ne)s parce qu'elle ne veut pas leur faire confiance est viciée et que ce pire des mondes imminent est non seulement terrifiant mais inhumain. Les machines y seront les indéfectibles alliées d'une police omniprésente et d'un état totipotent, et les êtres réduits à l'état de fragments et de nombres. Entités parfaitement connues et transparentes, supposées ne rien cacher. Car comment parvenir à cacher quelque pensée que ce soit à ceux qui connaitront le tréfond de nos innés et de nos acquis, de nos gènes et de nos *datas* ? Comment être encore « une cheville ronde dans un trou carré » ? L'une des réponses à la question est l'anonymat et la cryptographie. Faire en sorte de ne pas être identifié, ou tout du moins de ne pouvoir concaténer les bribes d'informations récoltées en un seul corpus de *datas* transparent. Il est indispensable aujourd'hui que quiconque se sent un brin « cheville ronde dans un trou carré », et quiconque fédère ou collabore avec d'autres chevilles, de crypter ses mails, le contenu de son disque dur, de vérifier le plus possible quelles sont les données dont disposent les prestataires de services auxquels il/elle a recours (fournisseur internet, banque, commerçants, assureurs, carte de fidélité, médecin, administrations et collectivité locales etc), et ce qu'ils en font.

Cela est nécessaire, mais sera-ce suffisant ? Je ne sais. Et je rêve de ce philosophe grec péripatéticien qui parcourait les villages en criant « j'ai des réponses, avez-vous des questions ? ».

Lagadu

(1) Expression métaphorique courante en anglais pour désigner des individus qui ne sont pas à leur place.
(2) Mémoire universitaire de Christiphe Naudin. http://mccccm.free.fr.
(3) Site du DRMCC http://mccccm.free.fr.
(4) « Les managers de l'Insécurité : production et circulation d'un discours sécuritaire », par Pierre Rimbert dans *La Machine à punir*, l'Esprit frappeur.
(5) ibid in *Les managers de l'insécurité* : « Xavier Raufer – Christian de Bongain de son vrai nom – est chargé de cours à l'Institut de criminologie de Paris [...] et responsable d'une collection aux Presses universitaires de France « Criminalité Internationale ». [...] Il a cosigné avec Alain Bauer le Que Sais-je *Violences et insécurité urbaine* (PUF) ».
6 – ibid – in *Les managers de l'insécurité* : « Alain Bauer enseigne à IHESI, Paris V-Sorbonne et Science Po.|...] Il intervient dans les modules sur les « violences urbaines » du CRMCC ».

Guerre contre la démocratie et la liberté

Tout au long de ces quatre dernières années, l'Union européenne a été le champ d'une bataille invisible et jamais rapportée entre d'une part, les exigences des agences de sécurité (agences de sécurité intérieure et extérieure, police, gendarmerie, douanes, services de contrôle de l'immigration...) et d'autre part, les fonctionnaires de l'Union européenne chargés de la protection des données (et soutenus par la Commission européenne). Au centre de ce conflit, se trouve la tentative d'assaut lancée par les agences de sécurité sur les lois de l'Union européenne relatives à la protection des données et de la vie privée au motif qu'elles feraient obstacle à leur besoin d'avoir accès à toutes les données échangées par des moyens de télécommunication. Selon les agences de sécurité, ces données devraient être conservées par les prestataires de service pendant une période s'étalant de un à sept ans et ces mêmes agences devraient pouvoir y avoir accès.

Les Directives européennes de 1995 et 1997 stipulent que de telles données ne peuvent être enregistrées que pour un seul motif : la vérification par le client de la liste détaillée de ses appels, après quoi ces données doivent être effacées ou rendues anonymes. Ces deux directives constituent le cœur même du droit à la vie privée au sein de l'UE et si celui-ci devait être remis en cause (garder une trace des données pour des raisons policières), cela le détruirait fatalement. L'histoire commence en 1993.

Les origines

Du temps de la guerre froide, d'énormes sommes ont été affectées par les Etats-Unis au NSA, et par le Royaume-Uni au Government Communications Headquarters (GCHQ) afin de mettre en place un système global de surveillance au profit des institutions militaires et de renseignement. Ce programme a débuté avec l'Accord dit UKUSA de 1948. Plus tard, au début des années 1980, ces mêmes institutions ont étendu leur réseau de surveillance grâce au système Echelon, afin de couvrir de façon encore plus étroite le renseignement politique et économique. Les agences de sécurité n'ont pas eu accès à ce système de renseignement, si ce n'est de façon tout à fait exceptionnelle, lorsque leur aide était jugée nécessaire. Les pouvoirs des agences de sécurité étaient alors définis par les différentes législations nationales, autorisant les interceptions des télécommunications et des postes sous réserve d'obtenir un mandat ou un ordre des juges et concernant un individu, une entreprise, une organisation ou un bâtiment précis. Bien entendu, les écoutes téléphoniques illégales se sont multipliées et dans la plupart des pays, les chiffres relatifs aux écoutes téléphoniques opérées par les agences de sécurité intérieure ont rarement été publiés.

Toutefois, au début des années 1990, il devint évident que l'on entrait dans une nouvelle ère des télécommunications avec l'apparition du téléphone mobile. Apparition qui présentait non seulement un nouveau défi pour les agences de sécurité mais surtout une nouvelle opportunité. Avec la chute du Mur de Berlin en 1989 et la disparition de la menace du communisme soviétique, de nouvelles menaces sont apparues. Plus précisément, des menaces déjà existantes ont été re-qualifiées en nouvelles menaces telles que le « crime organisé » ou « l'immigration illégale ». La fin de la menace soviétique a de plus atténué l'adhésion des gouvernements occidentaux au respect des normes démocratiques et des libertés civiles dans leur propre pays (à l'étranger, d'autres valeurs avaient cours comme par exemple le soutien de l'Occident aux régimes autoritaires à la condition qu'ils fussent anti-communistes). Sur le front intérieur, « la loi et l'ordre » (et non les droits et les libertés civiles) devinrent une question politique (et électorale) dominante. Les nouvelles « menaces » et la politique de « la loi et l'ordre » surgirent pour se poser contre les normes démocratiques et libérales qui avaient pourtant été mises en place à la fin des années 90 (les directives européennes étaient entrées en vigueur en 1995 et 1997).

À l'été 1993, le FBI a réuni plusieurs Etats membres de l'UE pour débattre de la question émergeante, non pas seulement de savoir comment surveiller les nouveaux moyens de télécommunication, mais comment les utiliser pour qu'ils soient profitables aux agences de sécurité concentrant le renseignement (en y incluant le « trawling »). Aussi bien les hauts fonctionnaires, que la police et les représentants des agences de sécurité intérieure ont dû faire face à deux problèmes. Le premier a été de savoir comment inciter les industries de la télécommunication à fabriquer de nouveaux matériels et logiciels qui permettent l'interception (dont l'interception en « temps réel » de plusieurs séries de communications se tenant entre deux pays ou plus). Le second problème a été de s'assurer qu'ils disposaient bien du pouvoir juridique de procéder à des interceptions sans restriction (et pas uniquement avec des mandats individuels ou grâce à des autorisations judiciaires).

La rencontre de 1993 au Quartier général du FBI à Quantico fut appelée « Séminaire sur l'application du droit international des télécommunications » (ILETS) et se tient depuis lors tous les ans. En octobre 1994, le Congrès des Etats-Unis adopta un projet de loi inspiré par le FBI exposant les « exigences nécessaires pour les utilisateurs internationaux » (IURs ou Requirements) pour pouvoir procéder à des interceptions de télécommunications. On supposait par là que ces textes façonneraient les normes internationales applicables à la nouvelle génération de matériels et de logiciels. Devant le danger de se retrouver à la traîne des Etats-Unis, l'UE a adopté un texte le 17 janvier 1995, sans d'ailleurs consulter un seul Parlement (qu'il soit européen ou national), et sous la forme de ce que l'on appelle la « procédure écri-

> L'ordinateur central de la sûreté américaine est incapable de faire une recherche avec deux mots clés; si un agent veut savoir ce que la mémoire policière contient sur les écoles de pilotage, il doit effectuer deux opérations, une avec «school», l'autre avec «flight».
>
> ROBERT MUELLER, DIRECTEUR DU FBI, DEVANT LA COMMISSION JUDICIAIRE DE SÉNAT

te » (le texte, au lieu d'être formellement adopté par le Conseil des ministres, a simplement été mis en circulation et approuvé). Cette action de l'UE n'a été rendue publique qu'en novembre 1996 lorsqu'un *Memorandum of Understanding* a été soumis à la signature des pays hors Etats-Unis et Union européenne. Les adresses auxquelles les signatures devaient parvenir étaient soit le Conseil de l'Union européenne à Bruxelles, soit le FBI aux Etats-Unis, d'où le nom donné à l'initiative : « le système UE-FBI de surveillance des télécommunications ».

Enfopol 98. En septembre 1998, le groupe de travail sur la Coopération policière au sein de l'UE a débattu puis approuvé une nouvelle volée de Requirements afin de couvrir les communications satellites et Internet. Les résultats prirent le nom d'Enfopol 98 et furent connus du grand public grâce à des fuites largement diffusées sur Internet. La couverture médiatique qui suivit la découverte contraignit les autorités à mettre cette initiative au placard jusqu'en 2001. Lors du Conseil de l'Union européenne du mois de mai consacré à la Justice et aux Affaires intérieures, les ministres approuvèrent un rapport expliquant bien clairement les conséquences des Requirements au sein de l'UE ; car en effet, ce qui est à présent connu sous le nom d'Enfopol 29 de 2001 a en fait incorporé toute la substance de l'Enfopol 98 de 1998. Bien qu'il mette en place des mesures encadrant les interceptions (dont la surveillance en temps réel), Enfopol 29 est toujours limité par la nécessité d'obtenir un ordre spécifique autorisant l'écoute sur un sujet précis.

Les fonctionnaires de la Commission en charge de la protection des données se prononcent contre les demandes. Les fonctionnaires de la Commission en charge de la protection des données étaient tout à fait conscients des exigences des agences de sécurité, formulées lors de forums internationaux comme dans le sous-groupe du G8 consacré au crime High-Tech afin que les données soient automatiquement conservées et que les agences de sécurité puissent les consulter pendant des mois, si ce n'est des années. Les exigences des agences de sécurité de l'UE sont présentées en détail dans un rapport envoyé par le NCIS (Service britannique du renseignement criminel) au Ministère de l'Intérieur en août 1999, détaillant les mesures envisagées dont, si nécessaire, la création d'un « site d'archivage de données ».

L'opposition formulée par les fonctionnaires de la Commission en charge de la protection des données à l'encontre des demandes des agences de sécurité de l'UE est soutenue par le groupe de travail de l'UE sur la protection des données et par la Commission européenne. Aussi, la seule route encore praticable pour les agences de sécurité était de passer par le Conseil de l'Union européenne.

La résistance des agences de sécurité

Le mouvement vers le Conseil a été amorcé par une proposition de la Commission européenne sur « le traitement des données personnelles et la protection de la vie privée dans le secteur des communications électroniques » (COM (2000) 385 final, 12.7.2000). La proposition a pour intention de mettre à jour le droit communautaire par la directive 97/55/EC mais elle n'a pas « l'intention d'apporter des changements substantiels à la directive existante », mais plutôt vocation à « mettre à jour les dispositions existantes ». La proposition se construit ainsi à partir des principes de la directive de 1997 et de son fondement qui se trouve dans la directive européenne de 1995 sur la protection des données inscrite dans le droit communautaire.

La proposition a été soumise au Parlement européen au cours de l'été 2000, car elle doit selon le principe de codécision, obtenir l'accord non seulement du Conseil et de la Commission, mais aussi du Parlement. Les rapporteurs parlementaires ignoraient jusqu'en avril 2001 que le Conseil entendait non seulement adopter Enfopol 98 (aujourd'hui Enfopol 29), mais débattait aussi d'un ensemble de projets de « Conclusions » appelant la Commission à amender la proposition ainsi que toutes les directives de l'UE existantes afin de satisfaire aux exigences des agences de sécurité de l'UE. De plus, il était entendu d'adopter un projet de « position commune » sur cette nouvelle proposition avant que cette dernière ne passe en première lecture devant le Parlement européen (appelées « lignes de conduite », elles ont été adoptées au Conseil sur les Télécommunications le 27 juin 2001).

Le changement proposé par le Conseil et apporté à l'initiative de la Commission semble mineur, mais il conférerait aux gouvernements de l'Union européenne et à leurs agences de sécurité tous les pouvoirs dont ils auraient besoin pour adopter des lois de mémorisation des données au niveau national (le dixième alinéa autoriserait « la conservation des échanges de données et de localisation de celles-ci pour une période limitée »). Avant tout cela, c'est le 7 juin 2001 que le Président du Groupe de travail sur la protection des données s'était adressé aux trois

Big Brother Awards. Sanctionnez les !

Cette année, les BBA (Big Brother Awards) sanctionnant les atteintes à la vie privée – de plus en plus nombreuses en ces temps de « guerre contre l'insécurité » – seront dissociés de la zelig.rc2. La remise des trophées 2002 aura lieu fin janvier 2003.
Ils seront décernés par un jury de personnalités, parmi lesquelles des juristes, sociologues et militants associatifs et des représentants de la FIDH (Fédération International des Droits de l'Homme) de la FIL (Fédération Informatique et Libertés).
Pour ce faire *Privacy International*, ONG organisatrice des ces BBA, vient de lancer un appel à candidatures. Vous êtes donc invités à nominer vos « big brothers » et aussi ceux qui ont le mieux défendus la vie privée, qui recevront des Prix Voltaire.
Par courrier ou ligne sur le site http://www.samizdat.net/bba
>> http://www.bigbrotherawards.eu.org

Richard M. Stallman. Pouvez-vous faire confiance à votre ordinateur ?

De qui votre ordinateur devrait-il recevoir ses ordres ? La plupart des gens pensent que leurs ordinateurs devraient leur obéir, et n'obéir à personne d'autre. Avec un plan qu'elles appellent « Trusted Computing » (« L'informatique de confiance »), de grandes sociétés de médias (dont celles du cinéma et de l'industrie du disque), ainsi que des sociétés d'informatique telles que Microsoft et Intel, prévoient d'agir pour que votre ordinateur leur obéisse plutôt qu'à vous. Des logiciels propriétaires ont déjà inclus des dispositifs malveillants, mais ce projet rendrait cette pratique universelle, au détriment de la liberté des utilisateurs. Richard Stallman, un des leaders du mouvement du logiciel libre, analyse les danger du système Palladium&TCPA dans un article disponible sur le web en traduction française.
>> http://www.zelig.org/article.php3?id_article=1

Windows. Se faire rembourser

Vous avez acheté un ordinateur pour l'utiliser avec GNU/Linux, un système libre de type BSD, ou GNU/Hurd, voir une version déjà en votre possession de Windows™ (c'est limite !), ou toute autre système d'exploitation, mais sur cet ordinateur qui vous intéressait était préinstallée une version de Microsoft Windows™ que le vendeur a refusé de désinstaller et rembourser. Ou bien, vous souhaitez tout simplement acheter un ordinateur sans Microsoft Windows™, ni aucun autre logiciel payant preinstallé... C'est votre droit ! Le Centre de détaxe Windows vous informe sur la procédure à suivre pour se faire rembourser et éviter ainsi de payer la taxe sur l'information levée par Microsoft. Les vendeurs n'apprécient pas, mais c'est parfaitement légal.
>> http://www.linux-center.org/detaxe/detaxe.html

Fournisseurs. Demander des comptes

Mon fournisseur d'accès ou hébergeur respectent-ils ma vie privée ? La Fédération informatique et libertés (FIL) recommande à chacun d'écrire à son FAI (fournisseur d'accès à l'Internet) pour lui demander de préciser sa position en matière de rétention des données de connexions à l'Internet et, le cas échéant, les modalités de fourniture aux autorités judiciaires des données et informations concernant les connexions et le courriers électroniques. Une initiative importante face aux mesures dangereusement liberticides contenues dans la LOPSI (loi Sarkozy). Les juristes de la FIL ont rédigé une lettre type que chacun peut reprendre à son compte et personnaliser pour son FAI.
>> http://www.lafil.org/act22

institutions européennes, leur disant entre autres choses : « une conservation systématique et préventive des communications ou de tout autre moyen de transfert de données des citoyens de l'Union européenne minerait les droits fondamentaux à la vie privée, à la protection des données, à la liberté d'expression, à la liberté et à la présomption d'innocence. La société de l'information pourrait-elle encore se réclamer société démocratique en de telles circonstances ? ».
Le 11 juillet 2001, le Comité des droits et libertés des citoyens a adopté son rapport sur ladite proposition par 22 voix contre 12 (la plupart des Eurodéputés socialistes – PSE – votant contre). Ce rapport propose que l'alinéa 10 soit modifié afin de limiter la conservation de données à des cas individuels spécifiques (comme à présent) et déclare : « la surveillance électronique à grande échelle, exploratoire ou générale, est prohibée ». Ce rapport devait être soumis au Parlement européen lors de sa séance plénière au début du mois de septembre. Si ce rapport devait être adopté sans amendement (et nous n'en avons aucune garantie), alors le Conseil se trouverait en porte-à-faux avec le Parlement européen et la Commission européenne.

Fin de partie
La résolution de ce problème marquera profondément non seulement les lois de l'UE sur la protection des données et les pouvoirs des agences de sécurité, mais ce sera aussi un important moment pour la démocratie au sein de l'UE. Soit la seule et unique raison pour conserver des données se maintiendra, soit elle tombera, mais sur cette question il ne saurait y avoir de « dérobade » ou de « compromis » bruxellois.
Cette fin de partie présente un autre tour inattendu. Le rapport du NCIS envoyé au Ministère britannique de l'Intérieur en 1999, ne l'a pas seulement été au nom des agences de sécurité mais aussi des agences de renseignement comme le MI5, MI6 et GCHQ. Il se pourrait bien aussi que ces agences souhaitent bénéficier des nouvelles formes d'interception qui permettraient d'avoir un accès direct à la source et à la suite de cela à la surveillance de type trawling. Ainsi, certains commentateurs débattent, que le moment venu, Echelon puisse être supplanté par de nouvelles technologies de surveillance qui émergeront si les gouvernements de l'Union européenne (et les Etats-Unis) poursuivent leur chemin. Dans le processus de globalisation, les exigences des lobbies surfant sur la vague « la loi et l'ordre », quand mises en balance avec les droits et la vie privée des citoyens, sont proches de l'emporter. Seule une forte résistance démocratique peut contrecarrer de telles perspectives mais ceci, en Europe, est rien moins que certain.

Tony Bunyan
Traduction : Nicolas Wuest-Famôse

Tous les documents cités en référence et bien d'autres encore sont disponibles sur le site Internet *Statewatch Observatory on Surveillance* in Europe (SOS) : www.statewatch.org/soseurope.htm

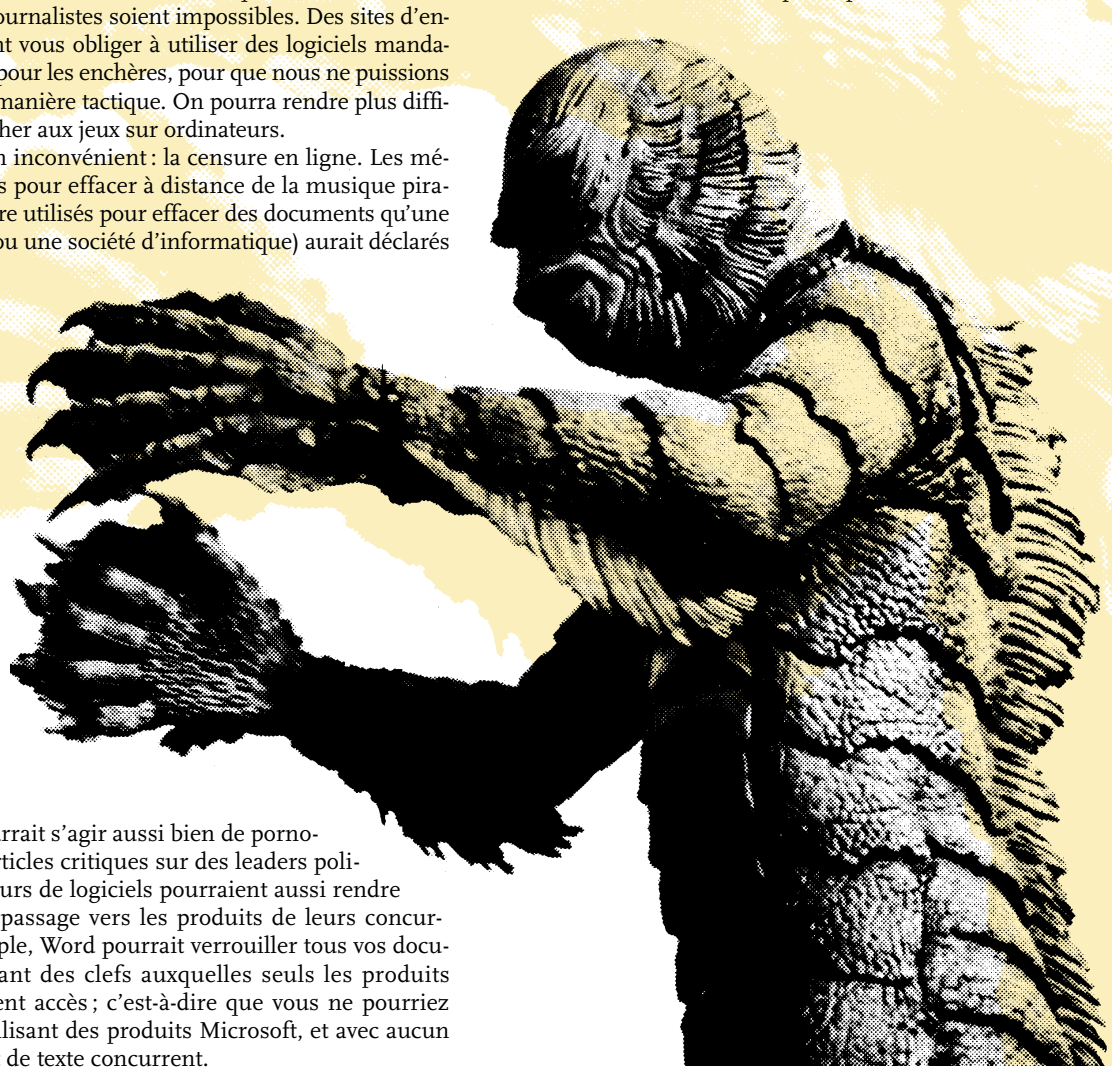
TCPA&Palladium – FAQ – Extraits

Qu'est ce que TCPA et Palladium ?
TCPA, qui signifie « alliance pour une informatique de confiance » (*Trusted Computing Platform Alliance* en anglais), est un projet dévéloppé par Intel. « Une nouvelle plate-forme informatique pour le prochain siècle qui améliorera la confiance dans le monde PC », tel est l'objectif d'Intel. Palladium est un logiciel que Microsoft déclare vouloir incorporer dans les futures versions de Windows ; il s'installera sur des machines TCPA et y ajoutera quelques fonctionnalités supplémentaires.

Concrètement, à quoi servent TCPA et Palladium ?
Ils fournissent une plate-forme informatique sur laquelle vous ne pouvez pas toucher aux logiciels, et où ces logiciels peuvent communiquer de manière sécurisée avec l'éditeur. La « gestion numérique des droits » (DRM ou digital rights management) en est l'application la plus évidente : Disney pourra vous vendre des DVDs qui seront décodés et lus sur une plate-forme Palladium, mais que vous ne pourrez pas copier. Les maisons de disques pourront vous vendre de la musique en ligne que vous ne pourrez pas échanger. Ils pourront vous vendre des CDs que vous ne pourrez écouter que trois fois, ou bien seulement à votre anniversaire. Toutes sortes de nouvelles variantes marketing deviennent possibles.
Il sera beaucoup plus difficile avec TCPA/Palladium d'utiliser des logiciels sans licence. Les logiciels piratés pourront être détectés et effacés à distance. À côté de la vente, la location des logiciels sera facilitée ; et en cas de cessation du paiement du loyer, non seulement le logiciel ne fonctionnera plus mais peut-être aussi les fichiers qu'il a créés.
Il y a beaucoup d'autres applications. Les gouvernements pourront faire en sorte que des documents Word créés sur les PC des fonctionnaires « naissent classifiés » et que les fuites électroniques vers les journalistes soient impossibles. Des sites d'enchères pourraient vous obliger à utiliser des logiciels mandataires accrédités pour les enchères, pour que nous ne puissions pas enchérir de manière tactique. On pourra rendre plus difficile le fait de tricher aux jeux sur ordinateurs.
Il existe aussi un inconvénient : la censure en ligne. Les mécanismes conçus pour effacer à distance de la musique piratée pourraient être utilisés pour effacer des documents qu'une cour de justice (ou une société d'informatique) aurait déclarés injurieux ; il pourrait s'agir aussi bien de pornographie que d'articles critiques sur des leaders politiques. Les éditeurs de logiciels pourraient aussi rendre plus difficile le passage vers les produits de leurs concurrents ; par exemple, Word pourrait verrouiller tous vos documents en utilisant des clefs auxquelles seuls les produits Microsoft auraient accès ; c'est-à-dire que vous ne pourriez les lire qu'en utilisant des produits Microsoft, et avec aucun autre traitement de texte concurrent.

Donc je ne pourrai plus lire des MP3s sur mon ordinateur ?
C'est au logiciel qu'il reviendra de définir les règles de sécurité pour ses fichiers, en utilisant en ligne un serveur dédié. Media Player déterminera donc quels types de restrictions seront attachés aux titres protégés, et je m'attends à ce que Microsoft passe toutes sortes d'accords avec les fournisseurs de contenus, qui pourront expérimenter toutes sortes de pratiques commerciales. Vous pourriez recevoir des CDs au tiers du prix normal mais vous ne pourrez les lire que trois fois ; si vous payez les deux tiers restants, vous obtenez la totalité des droits. Vous pourriez être autorisé à prêter la copie numérique d'un morceau de musique à un ami, mais vous ne pourriez écouter votre propre exemplaire qu'après la restitution de la copie par votre ami. En fait, on ne pourra probablement plus du tout prêter de la musique. Ces règles rendront la vie difficile à certaines personnes ; une politique de zonage pourrait vous empêcher de regarder la version polonaise d'un film si votre PC avait été acheté hors d'Europe.

À quoi d'autre peuvent servir TCPA et Palladium ?
TCPA peut aussi être utilisé pour mettre en place des conditions d'accès plus restrictives sur des documents confidentiels. Une armée pourrait, par exemple, décider que ses soldats créeront uniquement des documents Word avec une étiquette de type « confidentiels » ou d'un type supérieur et que seul un PC TCPA ayant un certificat délivré par son agence de renseignement pourra les lire.
Les grandes entreprises pourraient disposer des mêmes facilités, pour rendre difficile toute dénonciation de pratiques illicites. Elles pourraient s'assurer que tous les documents de l'entreprise ne soient lisibles que sur leurs propres PC, sauf lorsqu'une personne dûment autorisée lève cette interdiction. Elles pourraient aussi créer des dates de péremption : elles s'assureraient, par exemple, que tous les courriels disparaissent après 90 jours, sauf décision explicite de les conserver. (Pensez combien ceci aurait été utile pour Enron, ou Arthur Andersen, ou même Microsoft pendant leur procès antitrust.)
La mafia pourrait utiliser les mêmes facilités : elle pourrait s'assurer que les feuilles de calcul détaillant les dernières livraisons de drogues ne puissent être lues que par les PC accrédités de la mafia, et disparaissent à la fin du mois. Cela pourrait rendre le travail du FBI plus difficile ; quoique Microsoft soit en discussion avec les gouvernements pour savoir si les policiers et les espions auront accès aux clefs principales. Mais dans tous les cas, le fait pour un employé d'envoyer par courriel un document à un journaliste sera plutôt inefficace, puisque le journaliste n'aura pas la clef nécessaire au décodage.



Comment TCPA peut-il être détourné ?
La censure est l'une des inquiétudes. TCPA a été conçu dès le départ pour rendre possible l'élimination centralisée de contenus piratés. Les logiciels piratés seront repérés et désactivés lors d'une tentative de chargement, mais qu'en est-il des chansons et des vidéos ? Et comment pourrez-vous transférer une chanson ou une vidéo que vous possédez d'un PC à un autre, sauf à pouvoir la radier sur la première machine ? La solution proposée consiste à ce qu'un serveur distant administre la politique de sécurité des logiciels utilisant TCPA, comme un lecteur multimédia ou un traitement de texte, et tienne à jour une liste des mauvais fichiers. Elle sera téléchargée de temps à autre et utilisée pour vérifier tous les fichiers que le logiciel ouvrira. Les fichiers pourront être radiés en fonction du contenu, du numéro de série de l'application qui les a créés, et selon d'autes critères.
C'est déjà terrible, mais les possibilités de détournement vont jusqu'à la censure politique, bien plus loin que l'intimidation commerciale ou la guérilla économique. Je suspecte qu'elle progressera petit à petit. D'abord, des forces de police bienveillantes recevront des ordres pour lutter contre la pornographie pédophile ou un manuel de sabotage de la signalisation des voix ferrées. Tous les PC compatibles TCPA effaceront ces mauvais documents, et peut-être les dénonceront. Puis un plaignant dans un procès sur des droits d'auteurs ou en diffamation, obtiendra un arrêt d'une juridiction contre un document injurieux ; peut-être que les scientologues chercheront à mettre à l'index le célèbre Fishman Affidavit. Une fois que les avocats et les censeurs gouvernementaux auront compris toutes les possibilités, nous serons submergés.
Le monde moderne commença seulement quand Gutenberg inventa l'imprimerie en Europe, ce qui permit de préserver et de répandre les idées même quand les princes et les évêques voulaient les interdire. Quand Wycliffe traduisit par exemple la *Bible* en anglais en 1380-1381, le mouvement Lollard qu'il avait fondé fut facilement démantelé ; mais lorsque Tyndale traduisit le *Nouveau testament* en 1524-1525, il put imprimer plus de 50 000 copies avant d'être rattrapé et brûlé vif. L'ancien régime en Europe s'effondra et le monde moderne commença. Les sociétés qui essayèrent de contrôler l'information devinrent moins compétitives, et avec l'effondrement de l'Union Soviétique, il semble que le capitalisme libéral et démocratique ait gagné. Mais aujourd'hui, TCPA et Palladium mettent en danger l'héritage inestimable que Gutenberg nous a légué. Les livres électroniques, une fois publiés seront vulnérables ; des tribunaux pourront ordonner qu'ils soient interdits et l'infrastructure TCPA fera le sale boulot.
Après les tentatives de l'Union Soviétique pour référencer et contrôler toutes les machines à écrire et les fax, TCPA tente de référencer et de contrôler tous les ordinateurs. Les implications en terme de liberté, de démocratie et de justice sont inquiétantes.

Ross Anderson
Traduction : Christophe Le Bars

VO : http://www.cl.cam.ac.uk/~rja14/tcpa-faq. html
VF (en version intégrale) :
http://www.lebars.org/sec/tcpa-faq.fr.html

Sortez couverts... ou comment passer outre la cybersurveillance

Le présent document – dont la version intégrale et les mises à jour seront disponibles sur le site *Bubrother* (1) –, est librement inspiré d'un texte cosigné par Ian Brown, un cryptographe et défenseur des droits de l'homme anglais et Brian Gladman, ancien « directeur des communications électroniques stratégiques » du ministère de la Défense britannique et de l'OTAN. Il ne s'agit donc pas d'un manuel de H4x0r$ ni de pirate informatique, mais d'un texte destiné au grand public et cherchant à recenser divers moyens de protéger sa vie privée.

La résistible ascension des anti-crypto. La cryptographie permet de s'assurer que seuls l'émetteur et le destinataire d'un message soient à même de pouvoir le consulter. C'est justement ce qui fait peur aux forces de l'ordre, et aux services de renseignements, et ce qui a incité le gouvernement à prévoir certaines mesures censées contrer l'utilisation de la cryptographie. Mais sans même utiliser la crypto, tout internaute est désormais placé, par défaut et par principe, sur écoute électronique : la loi oblige en effet les fournisseurs d'accès et de service Internet (FAI) à conserver les traces de nos communications électroniques pendant un an.Une fois de plus, on associe la crypto au terrorisme et aux criminels, quand bien même elle est surtout utilisée en matière de commerce et de signature électronique. En attendant, cela n'empêchera ni les défenseurs de la crypto et de la protection de la vie privée de continuer à chiffrer leurs communications. En toute légalité. Et sans danger. Les mesures prévues par la LSQ sont en effet toutes aussi inefficaces les unes que les autres, à mesure que l'on prend les précautions nécessaires.

Des parades à la cybersurveillance. Privilégier l'utilisation d'un webmail sécurisé « étranger » au courrier électronique de son FAI « bien français »... On n'utilisera d'adresse e-mail @hotmail, @yahoo, @caramail et autres @aol que pour être noyé dans la masse, recevoir tout plein de spams et risquer de voir un jour son e-mail piraté, détruit, revendu dans un package de « données personnelles » ou intercepté. On lui préférera no-log. org (qui permet, en outre, de se connecter à l'internet sans que vous ayez à décliner notre identité), ou, mieux, *hushmail.com*, ou *lokmail.net*, qui ont le notable avantage d'offrir la possibilité de chiffrer ses messages... On préférera s'y connecter par webmail (qui permet la consultation en ligne, via un navigateur, de son courrier), plutôt que d'utiliser un logiciel de courrier électronique (qui télécharge ledit courrier sur votre PC, et laisse donc des traces de son passage), d'autant que leurs webmail sont sécurisés. Ainsi, les données ne sont pas transmises « en clair », mais chiffrées (via les protocoles SSL-TLS, que l'on reconnaît grâce au fameux « s » de « https :// », ainsi qu'au cadenas fermé qui apparaît dans la barre d'état de votre navigateur) et ne sont donc ni lisibles ni interprétables dans les fichiers logs de son FAI. Des services comme mail2web. com – ou n'importe quel *anonymizer* sécurisé – permettent par ailleurs de consulter son courrier électronique en ligne via une connexion chiffrée et ce, quel que soit le serveur de messagerie utilisé.

Prendre soin de bien faire le ménage, et de bien ranger ses affaires... C'est une évidence qui semble avoir échappé aux législateurs, mais un document qui n'existe plus ne peut être exploité. Ainsi, a priori, quelqu'un qui se servirait de la crypto pour fomenter quelque chose de répréhensible aura probablement le réflexe d'effacer de façon définitive toute trace de telles communications (ce qui n'est pas le cas lorsque l'on se contente de « jeter à la corbeille » un document). De même qu'il existe des broyeurs pour détruire les documents papiers, il existe des logiciels d'écrasement sécurisé des données, tel qu'*Eraser* ou *Wipe* : pour plus d'infos sur les diverses techniques de sécurité informatiques orientées utilisateurs voir la traduction française du site security.tao.ca (2).
On ne saurait ainsi que trop conseiller, soit d'effacer les données les plus sensibles, soit de les masquer avec un programme de stéganographie (une fois qu'elles ont été chiffrées, la stégano étant loin d'être aussi sécurisée qu'on le prétend), soit de les stocker sur un support amovible (disquette, disque dur, CD-RW, mémoire amovible – ou *pocket disk*- – USB, etc.) que, idéalement, l'on prendra soin de chiffrer en se créant un coffre-fort électronique (ce que permettent les distributions Linux Mandrake et Suse (3), ainsi que le logiciel *Scramdisk* pour Windows) et/ou de conserver en-dehors de son logis, ou encore sur un serveur ftp, ou site internet, situé dans la mesure du possible à l'étranger. De telles mesures, à commencer par le chiffrement de tout ou partie d'un disque dur ne peut en attendant se concevoir réellement que dans le cadre d'une politique globale de sécurité.

Du bon usage de la crypto. Bien utilisée, la cryptographie forte (dont l'utilisation est légale en France, faut-il le préciser) est incassable. Bien assimiler le processus de création, de conservation, de signature (afin de s'assurer de l'identité de ses correspondants) et d'utilisation des clefs est le B. A-BA de la protection de sa vie privée. Ne vous contentez pas, par exemple, de ne chiffrer vos e-mails que lorsque vous avez vraiment quelque chose à protéger -ce qui reviendrait à tirer la sonnette d'alarme, en tout cas si vous êtes surveillé-, alors qu'a contrario, une utilisation régulière permet de bien en assimiler le processus (de ne pas oublier le mot de passe, aussi), et ne peut qu'inciter vos correspondants à se metter eux aussi à la crypto. Par ailleurs, n'hésitez pas -mais vraiment pas- à lire les manuels... et pour bien commencer, allez sur *OpenPGP en français* (4).

Une chose est de se protéger, une autre est de protéger ses correspondants... Quand bien même cela est pratique, on prendra soin d'éviter de chiffrer les messages que l'on envoie à ses correspondants de sorte que l'on puisse soi-même les déchiffrer. Sous peine de piéger, à son insu, celui à qui l'on a écrit même si, et surtout si, vous n'êtes pas accusé (la jurisprudence, tout comme les traités internationaux, interdisent en effet l'« autoincrimination »). De même, vous pouvez être amené à déchiffrer un message qui vous a été envoyé, et perdre ainsi l'usage de vos clefs, sans parler de ce que vous pourriez causer d'ennuis à votre correspondant, voire à vous-même.
Changer régulièrement de clef permet de pallier, en partie, au risque de l'obligation de déchiffrement prévue par la LSQ. Il est en effet possible de donner une date d'expiration à sa clef (ce qui est vivement conseillé : 2 ou 3 ans est une bonne durée), et une clef périmée ne peut plus servir à déchiffrer les messages qui ont été chiffrés pour elle. De même, il est possible de « révoquer » sa clef, si l'on estime être en danger de devoir la révéler. L'utilisation de clefs à usage unique peut aussi y remédier. Il est en effet tout à fait possible d'envoyer à son correspondant un e-mail chiffré comprenant le message à protéger, ainsi qu'une nouvelle clef publique. Ce dernier n'aura qu'à répondre, et rajouter lui aussi une nouvelle clef publique, qui vous servira à répondre. Vous n'aurez plus qu'à révoquer, sinon détruire, la pre-

Fichage policier. Faites valoir vos droits !

Nous connaissons tous l'existence des fameux fichiers RG (Renseignements généraux). Mais connaissez-vous le STIC (Système de traitement des infractions constatées) ? Et quid du SIS (Système d'information Schengen) et d'Eurodac ? Soutenu par des défenseurs des droits de l'homme, de la vie privée et des mouvements sociaux, le site http://renseignementsgeneraux.net – qui n'est pas le site officiel des RG – vise à inciter tout un chacun à faire valoir ses droits d'accès, de rectification, d'opposition, d'oubli (tous prévus par la Loi Informatique et Libertés de 1978) à ses fichiers SIS, STIC & RG. Le problème du fichage policier est en effet on ne peut plus d'actualité. D'une part parce qu'il y a de plus en plus de fichiers policiers. D'autre part parce qu'ils sont peu, mal, voire pas du tout contrôlés. Enfin, parce que très peu sont ceux qui en connaissent l'existence, et encore moins ceux qui font valoir leurs droits en la matière. Qui surveillera les surveillants ?
Le fichage des militants des mouvements sociaux (cf. le scandale du rapport « Gauche 2000 ») et « antimondialisations », et l'interconnexion des fichiers policiers au niveau européen, voire mondial, ont été officiellement relancés l'an passé. Et nombreux seraient ceux qui ne pourraient accéder à leurs fichiers pour cause... d'"atteinte à la sûreté de l'Etat » (sic). Méga-base de données policières légalisée l'été dernier après avoir illégalement fonctionné 6 ans durant, le recours au STIC a quant a lui été intensifié par la Loi sur la Sécurité Quotidienne, et alimente quotidiennement le Système français d'Information Schengen.
Or, en l'état, le STIC, fichier « à charge » transformant tout fiché en présumé suspect, recèle d'ores et déjà de nombreuses erreurs. Mais seul le fiché est habilité à le corriger, encore faut-il qu'il en fasse la demande... Les demandeurs d'asile, les sans-papiers, les militants franchissant les frontières en vue de manifester sont quant à eux soumis à l'interconnexion des fichiers policiers européens d'Europol et du Système d'Information Schengen, qui n'ont de cesse de s'«enrichir». Aussi invitons-nous toute personne étant potentiellement fichée par les RG, ainsi que tous ceux ayant eu affaire à la police ou ayant franchi quelque frontière pour des motifs politiques, à faire valoir leurs droits en matière de fichage policier, d'informatique et de libertés.

Modèle de courrier à adresser par vous-même à la CNIL

Nom Prénom
Adresse
Date et lieu de naissance (1)

à Monsieur le Président
Commission Nationale de l'Informatique et des Libertés
21, rue Saint Guillaume, 75007 Paris

OBJET : *Demande de consultation des fichiers RG, STIC & SIS*

Monsieur le Président,
Conformément à la loi du 6 janvier 1978, je souhaiterais avoir accès aux informations me concernant inscrites dans les fichiers :
• *des Renseignements Généraux de* [DÉPARTEMENT(S)] (2)
• *du Système de Traitement des Infractions Constatées*
• *du Système d'Information Schengen*

[FORMULE DE POLITESSE AU CHOIX]

(1) Il n'est pas nécessaire de joindre une photocopie de votre carte d'identité à ce courrier.
(2) Nom du ou des départements où vous pourriez avoir été fiché par les Renseignement généraux.

mière clef, et répondre avec vos nouvelles clefs. Ainsi de suite. Le pseudonymat « en chaîne » permet enfin, a priori, de se protéger de toute dénonciation forcée (cybercafé + anonymizer + webmail situé à l'étranger, par exemple), de même que l'utilisation de remailers anonymes permet d'émettre un message (chiffré ou non) sans pour autant permettre de remonter jusqu'à la source du message (mais sans possibilité de répondre, aussi). Cela dit, et on n'aura de cesse de le répéter : l'anonymat sur l'internet n'existe pas.

La sécurité est un droit fondamental. Bruce Schneier, l'une des personnalités les plus respectées de la sécurité informatique, n'a de cesse de le répéter : la sécurité est avant tout un processus, une façon de se comporter, des réflexes, une culture… Aucune solution n'est fiable à 100 % : rien ne sert, par exemple, d'installer une porte blindée si on laisse la fenêtre ouverte. Ainsi, l'utilisation d'un logiciel de cryptographie ne sert à rien si elle repose sur une mauvaise gestion du mot de passe (pas assez long, facilement devinable, mal choisi, inscrit sur un bout de papier « caché » sous le clavier, etc.)… ou si l'on s'en tient à un OS comme Windows. Et si la cryptographie est relativement simple d'utilisation, il existe de nombreux moyens de la prendre en défaut. Autant dire que l'utilisation de la cryptographie ne peut faire l'économie d'une bonne politique de sécurité informatique : utilisation d'un *firewall* (surtout lorsque l'on dispose d'une connexion à haut débit), d'un anti-virus voire d'anti-troyens… Une chose est de se protéger de la cybersurveillance à même le réseau, une autre est de sécuriser son ordinateur de sorte que même si quelqu'un venait à y accéder (à distance ou non), et cherchait à l'étudier, il ne puisse l'exploiter. Comme le rappelle l'article 1er de la LSQ : « La sécurité est un droit fondamental. Elle est une condition de l'exercice des libertés et de la réduction des inégalités. » Sortez couvert…

Bugbrother

(1) http://www.bugbrother.com/archives/sortezcouvert.html
(2) http://www.bugbrother.com/security.tao.ca
(3) De même qu'on privilégiera toujours un logiciel libre à un logiciel propriétaire, on ne saurait que trop conseiller de migrer sous Linux plutôt que de rester sous Windows, ou Mac (encore que ce dernier soit moins truffé de failles que ne le sont les produits estampillés Microsoft). L'installation d'une Mandrake 9, par exemple, est encore plus simple (et combien moins onéreuse) que celle de Windows XP, l'interface graphique de Linux s'est par ailleurs considérablement améliorée, KDE n'ayant ainsi rien à envier aux bureaux de Windows & Mac, dont on retrouve la majeure partie des fonctionnalités et logiciels (et même plus) sous Linux. Migrer sous un OS – « système d'exploitation » (sic) – « libre » est par ailleurs un geste, et un choix, politique : celui de ne pas dépendre d'un OS « propriétaire », qui plus est moins sécurisé, et plus facilement piratable.
(4) http://www.openpgp.fr.st

Le manifeste crypto-anarchiste

Cypherpunks (1) du monde, la technologie informatique est sur le point de fournir aux individus et aux groupes la possibilité de communiquer et d'interagir les uns avec les autres d'une manière totalement anonyme. Il est possible pour deux personnes d'échanger des messages, de traiter des affaires et de négocier des contrats électroniques sans jamais connaître le Vrai Nom, ou l'identité légale, de l'autre. La source des interactions sur le réseau sera hors de portée grâce au rerouting extensif de paquets d'informations cryptées et de boxes anti-intrusion qui exécutent des protocoles cryptographiques avec une garantie presque parfaite contre toute forme d'intrusion. La réputation jouera un rôle central, bien plus important même, dans les tractations, que les taux de crédit d'aujourd'hui. Ces évolutions altèreront complètement la nature des législations gouvernementales, la capacité à taxer et contrôler les interactions économiques, la capacité à garder l'information secrète et altèreront même la nature de la confiance et de la réputation.
La technologie de cette révolution – et il s'agira bien d'une révolution sociale et économique – existait en théorie depuis une décennie. Les méthodes étaient basées sur l'encryptage avec clé publique, les systèmes sécurisés interactifs de zéro-savoir, et différents protocoles de logiciel pour l'interaction, l'authentification et la vérification. L'accent avait été mis jusque-là sur les conférences universitaires en Europe et aux Etats-Unis, conférences étroitement surveillées par la National Security Agency (2). Mais Mais ce n'est que récemment que les réseaux informatiques et les ordinateurs personnels ont atteint une vitesse suffisante pour rendre ces idées réalisables en pratique. Et les dix ans à venir apporteront assez de vitesse supplémentaire pour les rendre économiquement faisable et pour qu'il soit essentiellement impossible de les arrêter. Les réseaux à haute vitesse, Numeris, les boîtes anti-intrusions, les cartes intelligentes, les satellites, les Ku-band transmitters, les ordinateurs pesonnels multi-MIPS, les puces de cryptage, sont quelques-unes des technologies en cours de développement qui permettront tout cela.
L'Etat essaiera bien sûr de ralentir ou d'arrêter la diffusion de cette technologie, en invoquant les nécessités de la sécurité nationale, l'utilisation de la technologie pour le trafic de drogue et l'évasion fiscale, et des craintes de désintégration sociétale. Bon nombre de ces motifs de préoccupations seront valides ; la crypto-anarchie permettra de faire circuler librement les secrets nationaux et de vendre des matériaux illicites ou volés. Un marché informatique anonyme rendra même possible de répugnants marchés d'assassinats et d'extortions. Divers éléments étrangers et criminels seront des usagers actifs du *CryptoNet*. Mais cela n'arrêtera pas la diffusion de la crypto-anarchie.
Tout comme la technologie de l'imprimerie a altéré et réduit le pouvoir des corporations médiévales et la structure sociale de pouvoir, les méthodes cyrptologiques altèreront fondamentalement la nature de l'interférence du grouvernement et des grandes sociétés dans les transactions économiques. Combinée avec les marchés émergeants d'informations, la crypto-anarchie créera un marché liquide pout toute sorte de matériaux que nous pourrons mettre en mots et en images. Et tout comme une invention apparemment mineure comme le fil de fer barbelé a rendu possible la clôture de vastes fermes et ranchs, altérant ainsi pour toujours les concepts de terre et de droits de propriété dans l'Ouest de la Frontière, la découverte apparemment mineure venue d'une obscure branche des mathématiques deviendra les pinces coupantes qui démentèleront le fil de fer barbelé qui entoure la propriété intellectuelle. Debout, tu n'as rien d'autre à perdre que tes clôtures de barbelé !

Timothy C. May
Traduit de l'anglais par Serge Quadruppani.

- Texte lu par l'auteur au *Cypherpunk Meeting* de septembre 1992. Une première version avait été discutée aux éditions de la *Hackers Conference* de 1988,1989 et 1990.

(1) Terme de jargon désignant ceux des hackers se consacrant aux questions de cryptographie.
(2) Agence fédérale du type DST qui a en charge (entre autre) aux Etats-unis la régulation et le contrôle de l'utilisation des outils logiciels de cryptage.

Zeene Ne Delu

Les femmes font tourner les machines

Confronter les clichés qui traînent à la réalité ambiante. Oubliez une part de ce que vous pensez des féministes et entrez dans le féminisme pragmatique, intellectue, l politique et pratique, surtout pratique parce que les crises successives, les guerres, les viols sont la réalité ambiante. Pour beaucoup il faut des raisons pour se se battre sur le terrain de l'égalité des sexes comme si jamais on ne pouvait regresser et revenir sur ce qui a été acquis. Je fais la vaisselle, tu travailles, alors qu'est ce que tu veux de plus. L'antisémitisme et le racisme étaient des histoires passées en France : regardez comme le naturel revient au galop, au détour des élections. Mais, je m'éloigne.

La nébuleuse ex-yougoslave était un territoire où le féminisme avait sa place et un écho dans les années soixante-dix. De grandes conférences se sont déroulées par là, le capitalisme d'état égalitariste leur avait fait une place, les études, le travail, l'égalité des femmes. Comme ici, celles qui se battent pour la féminisation des noms se prennent de face la violence installée, quotidienne faite aux autres femmes hors cadre, hors périph, les crises post-titisme, et la guerre, les guerres ont ramené les associations de femmes sur des terrains de luttes concrètes. Comme si le féminisme ne pouvait qu'être cantonné dans la lutte corporelle -corporatiste : pas pour aujourd'hui et remises à plus tard la redéfinition des genres, au bénéfice de tous, fendues et quequettes comprises. Attaquées, toujours, dans la chair, juste au corps… alors on reprend tout à zéro, on attaque par les fondamentaux.

Naissance de Zeene Na Delu

C'est dans ce contexte que naît *Zeene Na Delu*, (Femmes au travail). Après des années soixante-dix actives, d'autres groupes se forment dans l'après Tito, avant les guerres, dans l'axe Lubjana- Zagreb-Belgrade, d'abord en créant des hotlines contre les violences. Les guerres se succèdent avec leur cortège de violences sexuelles, de retour au fourneau et à l'effort de guerre : nourrir, soigner, et faire des soldats. Les rangs des associations féministes grossissent au fur et à mesure des exactions : groupes de soutien, soins, mais aussi pacifisme politique, antinationalisme, antifacisme (voir les femmes en noir par exemple). Les groupes de femmes serbes sous embargo se retrouvent isolés. Les aides massives aux groupes croates créent des tensions, les ONG sont omniprésentes, leur argent et leur impérialisme politique aussi. Les liens d'avant guerre se distandent, les communications téléphoniques sont coupées.

« Grâce à Zamir, un serveur alternatif mis en place par Eric, un objecteur de conscience américain vivant en allemagne depuis la guerre du Vietnam, tout le monde, associations de resistance, militants se sont mis à l'utilisation intensive du e-mail et du chat. L'e-mail commença à être utilisé partout comme la poste entre nous, Sarajevo, l'etranger, entre les villes et les campagnes, les liens très forts entre les groupes viennent de là. » nous dit Laurence, une Américaine co-fondatrice de *Zeene na delu*. « Les groupes avaient besoin d'argent, de contact et de formations et tout c'est fait comme ça, grâce entre autres aux *Electronic Witches*, un projet cyberféministe de formation aux ordis pendant la guerre ». Les guerres ont accentué les clivages, d'autant plus que comme nous l'explique, la voix pleine de colère Milica, l'autre pillier de *Zene na delu*, « on nous a délaissé, parce ce qu'on est serbes, alors forcément on est les fascistes, même nous des associations féministes, antifascistes… on n'a jamais été pour la guerre, on est pacifistes, anti-racistes, tu comprends ? » Et quand finallement on s'intéresse à elles, « la plupart des fonds allaient aux hommes dans les associations." Le concept de Zene na delu est parti de là. Plutôt que l'argent que recevaient les associations féministes aille à des hommes parce que la voiture ne démarre pas ou que la machine à laver est cassée, faire que le peu d'argent aille à des femmes. « On a alors commencé à faire un réseau économique pour valoriser les femmes et leur travail, les identifier etc. en créant un repertoire de 250 femmes dans différents métiers de services avec des noms feminisés comme doctoresse ou plombière ;-)) » Et le cyber lab qui nous interesse me direz-vous. Il arrive. « Les organisations internationales financent surtout des formations couture, coiffure et ordis pour les refugiés. Dans une situation de crise, *Zeene* pense plutot formation pratique, gros oeuvres et moyens de communication et d'information. » rappelle Laurence. Les premiers ateliers de l'assoce seront donc des cours de réparation d'electro menager et de mecanique, de menuiserie et de recyclage et la mise en place d'une imprimerie-maison d'édition « galactika- feministicka » qui publie des traductions et des textes originaux. Puis, elles créent une *mailing list* postale et une newsletter qui diffusent à plus de 7 000 exemplaires dans toute la région, dans le but de prolonger les liens, coordonner et informer.

Une frange du collectif est plutôt contre les ordis, tendance limite luddite et *old-school*. Mais bientôt, plusieurs associations se regroupent pour travailler contre le trafic sexuel par l'education et le travail. C'est dans le cadre de ce projet et grâce au dévouement d'une nouvelle generation de féministes enthousiastes et délurées – plusieurs membres du cyber lab font parties de groupes fameux, guess what man : l'ingénieure réseau joue de la guitare- que se monte que se monte le *cyberfem-lab*. Elles sont jeunes, elles sont sacrément remontées, et elles aiment les ordis… L'un des principes de Zene na delu, c'est que les cours doivent être gratuits et les formatrices payées. « Les femmes travaillent assez gratuitement comme ça, pour que nous fassions la même chose » ajoute Milica, depuis le petit appart qui accueille le cyber-lab « alors, même si c'est un arrachement pour moi qui vient plutôt de la scène dyi-non profit, je monte des dossiers et je vais chercher les fonds où ils sont. Les ONG sont les seules à ne nous avoir pas lâchés. On a besoin d'argent, on est obligé de faire avec. Il faut que notre activité dure. La situation ici est critique. Toi-même tu trouves étonnant le nombre de casinos dans la ville, les traffics ont germé de partout pendant l'embargo et celui des femmes est le plus florissant. Notre truc c'est l'égalité par le travail, si les femmes ont leurs revenus propres elles ne sont plus dépendantes de leurs familles, et avec les ordis, on ne veut pas faire des secrétaires, même si c'est par ça qu'on commence, on veut des admins-sys, des ingénieurs réseaux, des programmeuses. »

« Nous, on veut aussi des Nike »

Les membres du *cyber-lab* oscillent entre volonté individuelle de réussite personnelle et action-collective-conscience-politique, mues par l'envie de sortir d'une vie de crises successives : « C'est tentant, tout est là, je ne comprends pas ce que tu appelles l'alter-mondialisation », nous dit l'une d'entre elle « nous, on veut aussi des Nike, je ne comprends pas quand tu dis que ça te choque la pub MacDo à l'aéroport, j'ai des fois deux emplois et je suis obligée de rester chez mes parents, surement jusqu'à ce que je me marie, je ne peux pas avoir une vie autonome. J'ai étudié, je suis ingénieure, je gagne 25 euros par mois, on ne me propose que des postes de secrétaire. C'est vraiment difficile de rejeter ce qui commence à nous arriver, » dit-elle alors qu'on se balade dans le futur belgrade-chic – toute la ville est en travaux, mais des enseignes connues et des vitrines aux agencements et achalandements familliers commencent à envahir la ville aussi horrible, grise et « stalinienne » que vous pouvez l'imaginer qu'est Belgrade – « on en a marre de ne connaître que les privations ».

Entre la guerre et les crises économico-politiques qui les ont suivies, plus de 500 00 jeunes ont quitté le pays. Pour ceux qui sont restés, il est devenu quasi impossible de partir, et la situation locale est peu brillante, entre une jeunesse marquée par le nationalisme et une situation quotidienne catastrophique, il reste peu de place pour d'autres voix même si B92, la célèbre radio continue à émettre et des centres comme le Rex sont toujours hyper actifs. C'est surtout les médias commerciaux qui ont pris le dessus.

A ce tableau idyllique s'ajoute, en ce qui nous concerne ici, la main mise par Microsoft sur l'informatique locale. La tactique habituelle est en marche : les rues sont innondées de logiciels piratés à 0,20 euros, les fondations équipent les associations en matériel compatible avec *winwin* préinstallé, et les alternatives n'ont que peu le droit de citer. « On apprend l'info sur papier et avant d'en sortir on en voit pas la couleur des ordis » nous raconte l'une des profs du cyber-lab, une espèce de P.J. Harvey locale, « Résultat, on connaît tout sur le papier et quand on arrive à avoir des machines on se retrouve dans le monde windows et puis c'est tout. Les logiciels libres ça nous passe pas mal au-dessus de la tête, ne serait-ceque parce que vu la dérégulation qui fait rage ici, personne ne paye rien, et est à milles lieux d'imaginer ce qu'est une licence de logiciels, un logiciel libre ou quoi que ce soit. » La firme du gros Bill, a signé en juin 2001, un contrat d'exclusivité avec le gouvernement : en échange de l'engagement de *Micro$* à financer à hauteur de 8 millions de dollars le gouvernement s'est engagé à lutter (sic) activement contre le piratage et le marché noir de logiciels et à faire de l'entreprise tentaculaire son conseiller en matière technologique. Ainsi, c'est toute l'artillerie qui se déploîe : cours, conseils, logiciels, machines, consultants, et *spyware* tissent la toile stratégique de l'empire informatique.

« Les logiciels libres, on en entend parler que depuis très peu de temps, mais on est déjà débordées alors on fait avec ce qu'on a, comme on peut, on a vraiment beaucoup de boulot, l'atelier informatique ce n'est qu'une partie de notre travail. Alors oui au libre, mais on a besoin d'apprendre, d'avoir l'occasion de pratiquer ».

La Peg

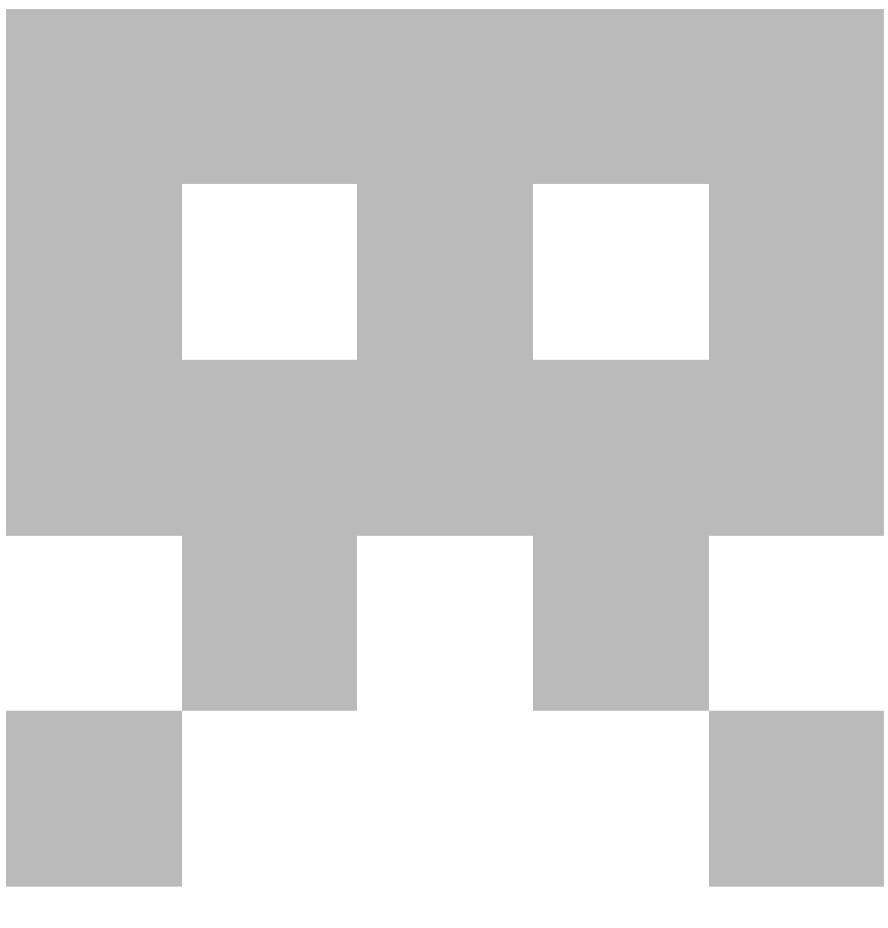
Digitales 2002.
Genres et nouvelles technologies

S'il est important d'attirer les femmes – et les rêves des jeunes filles – vers les sciences et les technologies pour qu'elles manipulent l'outil technologique, il ne faut pas qu'il devienne un nouvel instrument d'aliénation. Elles peuvent ouvrir un nouvel espace de réflexion et de création…Constant vwz nous présente son travail et ses réflexions cyberfeministes avant la conférence Digitales 2002 (du 4 au 7 décembre en Belgique) et son intervention à la Zelig.

>> http://www.zelig.org/article.php3?id_article=24

l'inform
veut êt

9-1



Une semaine d'ateliers, démos, rencontres, débats, autour des réseaux, de la communication, du logiciel libre et de la résistance électronique. Une semaine où l'on parlera de technique, de politique, de désirs, de créations, de mouvements...

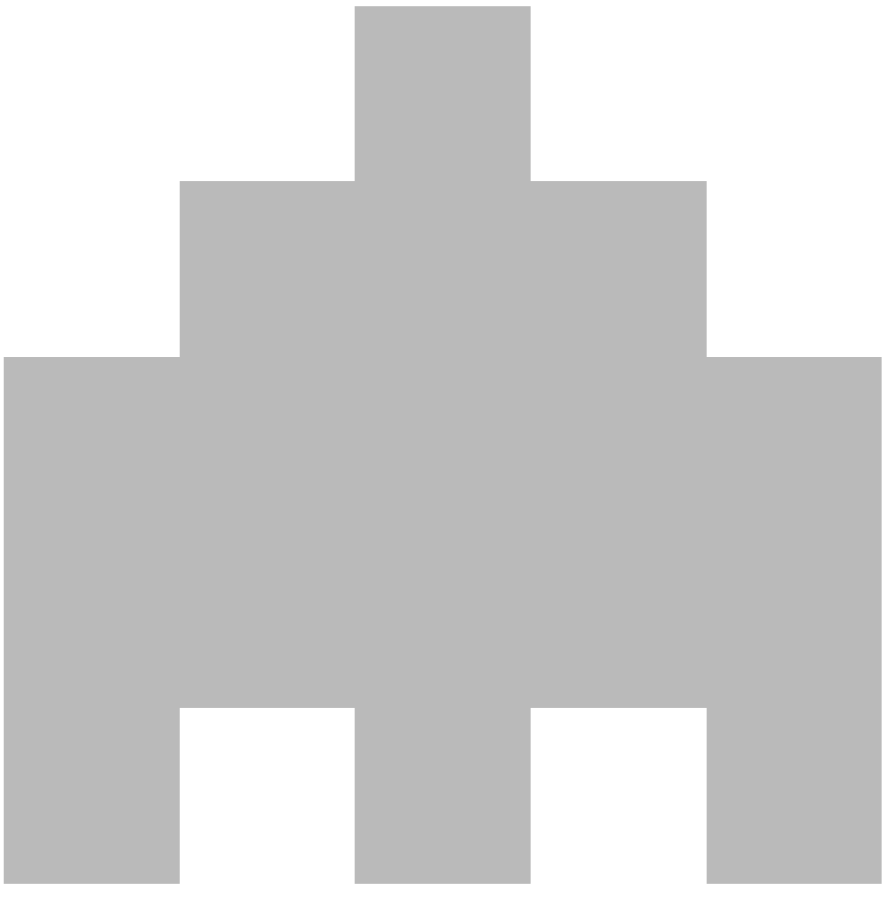
mation
re libre

Paris

-15 décembre 2002

http://www.zelig.org

activistes, cyberfeministes, militant(e)s,
syndicalistes, intellos précaires, nerds,
hackers, gender changer, cyborgs,
lowtech, mutant(e)s, newbies, bad grrrls,
travailleurs immatériels, hacktivistes,
codeurs et codeuses, technojunkies,
hybrides, general intellect, cypherpunk,
etc.



zelig.rc2

Comment devenir une cyberféministe ?

En tant qu'initiatrice de Old Boys Network (www.obn.org) – la première alliance cyberféministe – et auteure de quelques documents ainsi que d'œuvres cyberféministe célèbres, je suis souvent confrontée aux requêtes de toutes nouvelles cyberféministes demandant (de fait) « Comment puis-je apprendre à devenir une cyberféministe? ». Curieusement, il ne semble pas se trouver d'autres FAQ ou de sites web traitant de ce sujet, donc voilà le mien.

CORNELIA SOLLFRANK

Le désir de définition

Au fur et à mesure que la question « comment-devenir » se pose, arrive en même temps quelques questions cruciales. La première est « Qu'est ce que le Cyberféminisme ? » avant que nous puissions savoir « Qu'est ce qu'un(e) Cyberféministe ? » et pour finir, mais ce qui est nullement négligeable, « Pourquoi tout le monde devrait vouloir être une Cyberféministe ? » Tous ces points vont de pair ; je vais essayer de vous montrer le chemin à suivre dans cette jungle pour vous rendre plus accessible ce monde sauvage et non exploré qu'est le Cyberféminisme. J'ai déjà donné une conférence intitulée « La vérité à propos du Cyberféminisme », à Bruxelles, en 1999 pour le Festival des Jonctions. Dans cette conférence j'expliquai comment et quand le terme a été inventé, quel en était son usage avant 1997. 1997 est une année cruciale pour le Cyberféminisme, car c'est cette année là que *Old Boys Network* – OBN – a été fondé. Obn est la première alliance cyberféministe et a décidé de libérer le terme de son sens original ainsi que de développer une nouvelle stratégie visant à améliorer l'usage potentiel de ce dernier. Voici ce que j'entend par Cyberféminisme.

La première chose qu'OBN ait introduit est le refus d'une définition générale du Cyberféminisme. Cent antithèses ont été formulé lors du Premier Congrès International Cyberféministe à *Documenta X* (célèbre exposition d'art – NdT) à Kassel. Bien que cet acte était supposé montrer l'approche anti-idéologique d'OBN, beaucoup de personnes, à ce moment là, firent un amalgame sur le Cyberféminisme, comme pour tout. Ils pensaient que le Cyberféminisme n'était pas quelque chose de réel, de palpable, et que, par conséquent, il relevait d'un concept artistique pur. D'autres questionnai les buts politiques du Cyberféminisme, et comme la formulation était peu claire, ils nous accusèrent d'éviter le politique alors que le mouvement féministe a toujours été politique.

Dans un sens je pense que ne pas définir le terme était une bonne décision à priori, mais insuffisante, d'autant plus que le Cyberféminisme est un fait bien plus qu'une anti-chose. Je voudrais passer à l'étape suivante et vous apporter quelques définitions choisies, mais des définitions qui permettront toujours au Cyberféminisme d'être un concept ouvert, sans idéologie.

Définitions

–...

– Le Cyberféminisme est un modèle. Le terme fonctionne comme moment unificateur pour créer l'idée d'une identité politique sans avoir à lutter pour. (Cornelia Sollfrank).

– Le Cyberféminisme est le point d'entrée au problème actuel (Joseph Beuys).

[« Pour moi, il était important de placer les termes dans le décor ; il ne reste plus aux autres qu'à trouver ces termes intéressants. Ainsi ils fonctionneraient comme un point d'entrée au problème actuel ».]

– Le Cyberféminisme est un navigateur qui affiche le monde (Alla Mitrofanova).

– Le Cyberféminisme est un mythe (Yvonne Volkart).

L'idée du Cyberféminisme comme mythe a un grand potentiel. Pour citer Yvonne Volkart : « Un mythe est une histoire dont on arrive pas à identifier l'origine ou les différentes origines. Un mythe est fondé sur une histoire centrale qui est racontée encore et encore avec différentes variations. Cette caractéristique le rend actuel, le post-moderne en a besoin. Un mythe réfute UNE seule histoire comme étant l'*unique* vérité et implique une recherche de vérité dans les espaces, dans les différences des différentes histoires. Parler du Cyberféminisme comme un mythe ne revient pas à le mystifier mais signifie que le Cyberféminisme n'existe qu'au pluriel ».

Qu'est ce que çà veut dire « le Cyberféminisme n'existe qu'au pluriel ? » Simplement, qu'il nécessite un environnement de débat pour grandir. Il nécessite des structures dans lesquelles les voix peuvent être apportées ensemble – ces voix individuelles exprimant les Cyberféminismes.

Le contenu demande une forme

Ceci nous rapporte à OBN. Le *Old Boys Network* est dédié à la construction d'espaces virtuels et réels dans lesquels les cyberféministes peuvent rechercher, expérimenter, créer, communiquer et agir. Ces plates-formes fournissent une présence contextualisée pour des approches diverses et interdisciplinaires du cyberféminisme. En d'autres termes, les plates-formes telles que les conférences, rencontres, débats, sites Internet, listes de discussions sont nécessaires pour réaliser = créer une réelle construction. La réalisation du Cyberféminisme requiert d'autres cyberféminismes, des cyberféminismes différents.

Il appartient au Cyberféminisme de construire ses propres structures.

Le contenu Cyberféministe reflète toujours aussi les conditions de sa production, communication et distribution. Les positions plurielles qui partagent cette approche dans un même contexte, contribuent à sa structure. Les approches individuelles juxtaposées les unes aux autres, créent un contexte. Il n'y a pas *une seule* histoire vraie, un vrai Cyberféminisme. La vérité est dans la variété, la différence, dans les espaces entre les approches et les positions individuelles.

Pour illustrer cela, OBN a choisi que trois représentantes qui discutent de la même question pour montrer la variété de réponse possible dans le même contexte. La question n'est pas d'avoir raison mais plutôt une question d'analyse, de comparaison, de discussion, de combats et d'acceptation. C'est cela qu'OBN appelle la Politique de la dissidence (*Politics of Dissent*). (Egalement très utile pour éviter les conflits – comme nous le pensions.) Certains s'élèvent en disant qu'une politique de la dissidence ne peut pas exister, puisque la politique se définit elle-même clairement en exprimant des idées et des buts. C'est une (double) interprétation erronée puisque la politique de la dissidence nécessite un accord sur la structure ; en plus, l'organisation du désaccord est hautement politique même dans une politique traditionnelle. Le but commun se situe à un niveau différent, le niveau de l'organisation/structure. Sans accord sur la strucure rien (ne peut exister) n'existe.

Cyber

Cyber dans Cyberféminisme n'indique pas simplement quelque chose de nouveau, mais porte aussi sur les médias en réseaux numérique. Cyberféminisme sans *Cyber* ne serait pas possible. Les média en réseau et ses caractéristiques spécifiques en terme de simulation et de communication en sont une part intégrante. La position du sujet Cyberféministe est directement reliée à ce médium.

Féminisme

Féminisme dans Cyberféminisme indique une référence au féminisme, mais pas simplement une référence historique linéaire. Le genre est compris dans un sens étendu comme une catégorie politique classique, mais aussi connecté à une autre approche de la politique.

Politiques Cyberféministes

OBN comprend la politique comme une chose fonctionnant avec la confusion, la déception, l'irritation l'impatience et l'excitation. Les nouveaux espaces de pensées et d'action qu'OBN a ouvert ne sont pas rempli avec des instructions générales et des réponses. OBN ne formule pas des théories ou des thèses. Les Cyberféministes sont individuelles et donc, par la même, les stratégies cyberféministes continuent à être partiale, en cours d'élaboration et même à se contredire l'une l'autre. L'interprétation d'OBN sur la politique peut sembler paradoxale. Elle consiste à former des alliances, définir des problèmes et des différences communes, créer un débat ; c'est pragmatique, philosophique et actif ; rejetant les objectifs communs, comparant les stratégies, jonglant avec les différentes notions de la politique comme par exemple l'intention, l'idéologie, le jeux et l'anarchie. Cette version de la politique connaît son efficacité sans avoir à en parler. C'est tout un art.

Real Politique

On peut dire en deux mots que la politique c'est (l'organisation) des structures de pouvoir. Le germe de la politique est petite et se divise en unités plus petites encore, comme les cellules. Les membres doivent s'impliquer, doivent discuter de leurs idéaux, tester leurs limites ; les règles doivent être définies, les sanctions déterminées. Formation du sujet politique. La politique

est quelque chose de complexe et signifie la formation de relations et de société. Une recette simple ne peut pas exister. (Le Cyberféminisme prétend les avoir, mais au final refuse de les donner. C'est vipérin.) Les mauvaises compréhensions sont que la politique peut être simpliste et être pour ou contre quelque chose devient alors politique. C'est une réduction de ce qui est politique. Une nouvelle définition de la politique semble plus intéressante, élargissant les petites structures vers de plus grandes.

Le réseau/La Solution

Beaucoup de personnes n'ont pas de relation personnelle avec la politique. Le cyberféminisme, le réseau et l'auto-organisation peut aider. La création de structures parallèles permettent l'expérience personnelle de la politique. Devenir une « membre » – une Cyberféministe – nécessite de revenir à vous-même, votre intuition et pensée propre. C'est l'activité principale. Vous ne pouvez pas étudier et copier le Cyberféminisme, mais vous devez inventer le votre. Vous devez ensuite le rendre public, devenir une part du débat. La passivité et la consommation n'existe pas dans le Cyberféminisme. C'est l'option offerte par le Cyberféminisme – devenir pertinent.

Résultat

Un manuel *how to* est habituellement quelque chose de relativement simple. Il vous aide à accéder au sujet choisi, vous familiarise par les premiers pas. Vous avez des instructions et des définitions précises qui vous conduisent dans une nouvelle direction. Ce concept éveille deux questions en moi :

1. Est-ce que je veux que quelqu'un me donne des instructions ?
2. Est-il possible de donner des instructions simples pour des choses complexes – comme le cyferféminisme ?

Bien sûr, c'était un tour pendable pour vous faire croire que quelquechose comme un « manuel pour le Cyberféminisme » peut exister. Et l'astuce marche bien, puisque tout le monde est sensible aux recettes simples. Vous êtes donc ici en attente de mes instructions et je travaille dur pour vous décevoir... Ne serait ce qu'un tout petit peu, mais aussi, dans le même temps, j'espère vous faire comprendre « Comment devenir un(e) Cyberféministe ? »

Instructions pour les incorrigibles

1. N'essayez pas d'apprendre ce qu'est le Cyberféminisme – les interpretations qu'auront d'autres personnes n'est pas approprié pour les premiers pas.
2. Demandez-vous si vous désirez réellement devenir plus active que vous ne l'êtes déjà. L'activité principale du Cyberféminisme requiert que vous formuliez votre propre approche et que vous aidiez dans la construction de structures (tous ensemble nous avons beaucoup à faire).
3. Si votre premier travail de Cyberféministe est prêt (il n'y a aucun problème à ce que vous appeliez cela art, théorie, action ou quoi que ce soit d'autre), faites en contribution dans le contexte qui est le votre, mieux, à *Old Boys Network*.
4. Vous pouvez alors essayer doucement de commencer à comprendre les autres Cyberféminismes, penser à d'autres langues pour une meilleure communication.
5. En le faisant pendant quelques années, cela vous permettra de réaliser combien c'est fun mais beaucoup de travail d'être un(e) Cyberféministe et de changer le monde.

D'avantages de questions pour vous-même :

– Voulez-vous changer le monde ?
– Voulez-vous vous changer vous-même ?
– Voulez-vous faire carrière ?
– Voulez-vous devenir célèbre ?
– Savez-vous ce que vous préférez faire le plus au monde ?
– Savez-vous dans quoi vous êtes le/la meilleur(e) ?

Traduit par Lansciac & Nathalie Magnan

Manifeste cyberféministe pour le 21e siècle

Nous sommes le con moderne
L'anti-raison positive
Délivrées déchaînées impitoyables
Nous voyons l'art avec notre con
nous faisons l'art avec notre con
Nous croyons à la jouissance à la folie
à la sainteté et à la poésie
Nous sommes le virus du nouveau
désordre mondial
Nous brisons le symbolique de l'intérieur
Saboteuses de l'Unité Centrale du paternel
Le clitoris comme ligne directe de la matrice

LES VNS MATRIX

Terminatrices du code moral
Mercenaires de l'humeur visqueuse
Descendent sur l'autel de l'abjection
Sondent le temple viscéral prophétisent
dans des langues inconnues
Infiltrent interrompent disséminent
Corrompent le discours
Nous sommes le futur con

VNS Matrix
http://sysx.org/vns

Lettre ouverte au réseau Indymedia

Indymedia est un réseau ouvert, anti-hiérarchique, et structuré horizontalement. Contrairement aux médias de masse/institutionnels, Indymedia n'a que faire des profits financiers. Nous ne cherchons pas à nous substituer aux médias institutionnels, ni à combler les espaces vacants que ceux-ci laissent à disposition. Nous n'aspirons à aucune relation ou réconciliation avec ceux-ci.

Notre objectif n'est pas le « journalisme indépendant »
Par « journalisme indépendant », nous entendons ce type de journalisme qui contraste avec la tendance dominante du fait qu'il fournit une information de meilleure qualité. Ce journalisme peut avoir un contenu partiellement « anticapitaliste », mais n'embrasse en aucun cas cette philosophie comme base de départ.
Notre action anticapitaliste ne s'arrête pas à Indymedia. Au contraire, Indymedia en est le produit. Nous considérons Indymedia Thessaloniki comme partie de notre action globale. Il est important que nous invitions tout le monde à participer, à apporter des idées et opinions, mais aussi à impulser des actions de terrain, dans le but d'éviter la reproduction de deux rôles distincts : celui de journaliste d'un côté, d'observateur de l'autre. De telles tentatives ne peuvent qu'être de nature indépendante et anti-hiérarchique.

Mais que signifie « indépendant » ?
En aucun cas cela doit-il signifier « neutre politiquement ». Cela implique tout d'abord d'inciter les personnes autonomes et indépendantes à participer, car c'est là leur seul moyen d'assurer leur autonomie collective. Ces participations interactives doivent aller de paire avec la volonté de ces personnes de mettre en pratique des modes de vie auto-organisés.
La participation à Indymedia ne doit pas être considérée comme une dette à payer à un quelconque processus révolutionnaire, ni comme de la charité journalistique. Au contraire, cela devrait être vu comme un choix de vie conscient. En conséquence, nous voyons comme caractéristiques essentielles d'Indymedia sa structure horizontale anti-hiérarchique, et son indépendance financière et idéologique déterminée.
Indymedia doit non seulement rester indépendant des institutions, mais aller jusqu'à refuser la coopération avec les organisations institutionnelles et autres partis politiques. En tant que média « non autorisé », Indymedia se doit d'être contre les institutions officielles. Indymedia doit maintenir son opposition à toutes les formes de hiérarchie, non seulement dans son fonctionnement interne, mais aussi et plus encore dans une volonté d'étendre les pratiques anti-hiérarchiques à toute la société. Car il ne suffit pas de travailler ainsi au sein d'Indymedia, mais il s'agit de mettre ces idées en pratique tant dans son action politique que dans sa vie de tous les jours.
Nous voulons utiliser Indymedia Thessaloniki comme un espace (virtuel ou non) d'échange d'idées et d'informations, de communication entre groupes et individus de Grèce, des Balkans, d'Europe et au delà. Il s'agit pour nous d'une action de résistance contre le système capitaliste global et ses structures, l'humiliation et la suppression des personnes, la destruction de l'environnement, le sexisme, le racisme et le nationalisme. Nous pronons l'auto-organisation et la non-hiérarchie, l'action anti-autoritaire, la solidarité et la critique positive, dans une optique de libération sociale.
En ce qui concerne les liens entre Indymedia et les mouvements sociaux, nous pensons qu'Indymedia est le fruit d'un besoin des manifestant-e-s. Besoin d'une information différente, à l'opposée de celle des médias institutionnels, et libérée de l'emprise des « leaders » auto-proclamés de chaque mouvement.

Indymedia appartient à la base.
Indymedia ne peut être distinct des mouvements sociaux et des endroits (pays, rues, villes, centres sociaux, usines, forêts) où ces mouvements confrontent le pouvoir. Aucun mouvement n'est statique. Tous sont dynamiques, sujets à évolution, se renforcent ou s'affaiblissent, sont déterminés ou piégés par les promesses des dominants, combattent le système ou tentent de le réformer... et se transforment avec le temps. Les centre Indymedia qui sont coupés des évolutions de ces mouvements, qui n'affectent ou ne sont affectés par ces luttes, sont condamnés à l'isolement. En tant que partie du mouvement, Indymedia donne la possibilité de créer des communautés locales et globales, dont le potentiel est de devenir forces antagonistes.
Indymedia doit représenter un danger pour le système. Ainsi que le montre l'histoire, les autorités ont toujours tenté d'assimiler ce qu'elles ne pouvaient supprimer. Indymedia est visé (voyez la conférence *European Peripheral Magazines* à Lund, sponsorisée par le gouvernement suédois, et à laquelle des Indymedias ont accepté de participer).

Je m'inquiète pour le jour où, dans 10 ou 15 ans, ma fille me demandera : « Papa, tu faisais quoi quand ils ont censuré la liberté d'expression sur l'Internet ? » — Mike Godwin

Il est un point de vue largement partagé, selon lequel nous pourrions indirectement sensibiliser la population au travers des médias commerciaux, qui touchent une bien plus large audience, en leur communiquant des informations provenant d'indymedia (ce point de vue a été accepté par nombre de personnes de l'ensemble du réseau Indymedia européen, et a été introduit lors de la réunion européenne d'indymedia à Berlin, du 18 au 20 juin 2002).
A la question « acceptez-vous de faire de l'agitation anticapitaliste par le biais des médias dominants », il était souvent répondu que « de cette manière, nous parvenons à exploiter les médias ». Cet argument ne semble pas très convainquant, si l'on considère qu'il n'est pas facile de faire jouer les grandes entreprises médiatiques à notre jeu contre leurs propres intérêts. Ce point de vue naïf élude une question essentielle : pourquoi les médias commerciaux désirent-ils obtenir les informations d'Indymedia ? Il est clair que nos contenus sont opposés à ce qui anime les médias institutionnels et commerciaux. Le mode de fonctionnement d'Indymedia implique la fin des multinationales, des médias officiels et, bien-sûr, des structures de travail hiérarchisées.

La réponse n'est peut-être pas si évidente, après tout…
Enfin, les réseaux Indymedia ont-ils été créés pour communiquer leurs contenus aux médias institutionnels ? C'est la seconde chose qui nous semble contradictoire. Peut-être est-ce plutôt les médias officiels qui nous utilisent, et qu'ils tenteront de le faire de manière plus extensive à l'avenir ?
En somme, Indymedia peut être considéré comme un regroupement de collectifs de médias indépendants, de centaines de médiactivistes et d'organisations de base assurant une couverture non-commerciale et non-institutionnelle des événements politiques et sociaux majeurs. Nous voudrions vous inviter à une discussion ouverte sur Internet au sujet les différents thèmes que nous avons abordé. Nous pensons qu'il existe un potentiel énorme de développer Indymedia. En tant qu'initiateurs de la discussion, permettez nous de poser quelques questions, comme thèmes principaux de cet échange :

– L'un de nos soucis est le comportement d'Indymedia vis à vis des médias commerciaux, des organisations non-gouvernementales, des partis, etc.
– Une autre problématique d'égale importance concerne les aspects financiers et les diverses manières de financer et soutenir les activités (vente de vidéos, interviews, contributions libres…).
– Enfin, il y a beaucoup de débats autour du rapport d'Indymedia au mouvement anticapitaliste, et de la possibilité pour le réseau Indymedia d'être une composante essentielle de cette lutte, et pas seulement un outil.

Nous serons heureux d'entendre vos reflexions sur tous ces différents sujets.

Salutations militantes,
Le groupe éditorial d'Indymedia Thessaloniki (Grèce)
Adresse pour les réponses : imc-thessaloniki@lists.indymedia.org

Le texte précédent a été diffusé en juin 2002 à l'ensemble du réseau Indymedia, dans sa version anglaise. Traduit en français par Lettuce (lettuce@inventati.org), qui n'a aucun lien avec IMC Thessaloniki.

Ce document est disponible en anglais et au format HTML à l'adresse suivante : http://thessaloniki.indymedia.org/firstletter.php3

Mouvement et communica(c)tion

Au sein des dispositifs de mobilisation du mouvement « no-global » et plus généralement des mouvements sociaux, la communication via les réseaux électroniques joue un rôle évident. D'une certaine façon, Seattle fut autant la « révélation » d'un mouvement fait de multiples mouvements – le « mouvement des mouvements » comme il sera défini par la suite – que celle de l'émergence du modèle des « médias indépendants » dont les nombreux groupes locaux d'Indymedia, un peu partout dans le monde, sont le symbole le plus visible. De fait, le mouvement « no-global » fait preuve d'une impressionnante capacité à multiplier et combiner les canaux de communication où circulent non seulement de l'information, mais aussi du débat, des pratiques, des subjectivités et des capacités d'organisation. Le réseau est probablement le paradigme organisationnel des multitudes, et les agencements de communication sont (avec les initiatives transnationales de type contre-sommet) les instruments privilégiés de la coopération politique entre des milliers de réalités diffuses et dispersées. Car derrière le vocable confus et confusionniste de « médias indépendants », ce dont il est bien question c'est de la capacité désormais démontrée des molécules du mouvement à communiquer pour elles, à communiquer entre elles, tout comme à communiquer vers l'extérieure, en s'appropriant les outils de communication qu'offre l'Internet : combien de centaines de *mailing lists*, de sites web, de forum ou de bulletins électroniques, etc. (mais aussi d'émissions de radio ou de bulletins imprimés) se sont créés dans la continuité de Seattle pour communiquer Prague, Göteborg, Québec City, Bruxelles ou Gênes ? Autant de murmures qui composent le flot d'une communication effectivement indépendante, mais surtout qui se cherche des voies de traverses pour échapper au monopole et au balisage médiatique de l'information.

Des limites évidentes

Ce serait dans le même temps se mentir que d'en rester à un tel constat idyllique : si la communication *dans* le mouvement est l'une des forces de celui-ci, elle en exprime dans le même temps toutes les faiblesses. Si l'on regarde de plus près les contenus de cette communication en mouvement on doit concéder, qu'à côté d'une réelle capacité à contourner (même partiellement) la puissance d'occultation des médias *mainstream*, à côté d'une capacité à faire circuler de la subjectivité politique, elle reproduit aussi des séparations, des logiques de ghetto et des effets de brouillage évidents. « Médias indépendants » et « communication alternative » se limitent en effet trop souvent à la reproduction des faiblesses des milieux militants. en particulier :

- Confusion entre l'information et la propagande : trop de « news » publiés sur les sites d'infos, ou envoyées sur les mailing lists, ne sont jamais qu'un copier-coller de tract ou de communiqué, ou la lutte, les émotions, le vivant qui font la richesse des mouvements se perd dans le caractère autoréférentiel des formules et des slogans.
- Incessantes querelles sur le thème du « traître », des « réformistes » et des « faux révolutionnaires »… qui s'étalent dès qu'il y a un espace de libre expression (mailing lists, site web en *open publishing*) au point de grever grandement les possibilités réelles de communication et d'échange.
- Persistance des attitudes de « boutiques », chaque expérience de communication tenant finalement bien plus à son « label » qu'à la nécessité de produire de la coopération, qu'à la nécessité d'apprendre à être ensemble en mouvement avec nos spécificités et nos richesses (1).

Pour dépasser cette situation, rien ne sert de se lamenter, il nous semble qu'il est par contre grand temps d'ouvrir un débat – véritablement transnational, véritablement pluraliste – autour d'un certain nombre de questions politiques comme celle des *contenus* de la communication alternative, ou encore celle des *formes* et des moyens d'une véritable coopération entre les diverses réalités des « médias indépendants » et au-delà l'ensemble des activistes des réseaux. Cela suppose aussi sans doute d'avancer sur quelques clarifications politiques sur ce qu'est (et n'est pas) la communication alternative.

Médias indépendants ou communication alternative ?

Quel est le problème que nous posent les médias *mainstream* ? Est-ce uniquement leur dépendance envers les grands groupes financiers du secteur du spectacle, ou bien plutôt la *médiation* elle-même, cette fausse objectivité tant revendiquée par les médias pour couvrir d'un minimum de vertu la réalité de la chasse au scoop, de la soumission à l'Audimat et aux « taux de pénétration », ou encore de prima de la publicité. « En brouillant délibérément la frontière entre l'objectif et le subjectif […] le Média construit l'image d'une fausse subjectivité, emballée et vendue au consommateur comme un simulacre de ses propres « sensations » et « opinions personnelles » ou de sa subjectivité. Et en même temps, le Média construit (ou est construit par) une fausse objectivité, une fausse totalité, qui s'impose comme la vue-du-monde qui fait autorité, bien plus que n'importe quel simple sujet » (2).
Ce qui nous sépare finalement des médias c'est avant tout le point de vue à partir duquel nous tentons de produire de l'information et de la communication, la tentative de réduire la médiation (celle des experts, des spécialistes) à sa plus simple expression, en donnant les moyens à chacun et chacune, à toutes les réalités sociales auxquelles nous nous adressons, d'agir leur communication, de faire de la communication un moment de la lutte, de la mobilisation, du conflit. Encore et toujours la proposition d'une multiplication de « médias intimes » (3) contre les énormes machines de guerre de l'information spectaculaire.
Cela suppose donc plus qu'une simple altérité structurelle – que revendique le document d'indymedia Théssalonique (4) – mais bien d'inventer des modes polyphoniques (pluriels et pluralistes si l'on veut) pour produire de l'information, pour faire circuler le débat, et pour produire de la subjectivité. Quelque chose qui suppose une capacité à diffuser l'expertise et construire des espaces, tout comme à combiner la diversité et la coopération : et de fait il s'agit plus là d'alternative que d'indépendance…

L'au-delà de l'open publishing

Après Seattle le modèle Indymedia de l'*open publishing* – c'est-à-dire de la libre publication des textes, images et vidéos sur le web, sans filtrage préalable, et avec un minimum de « modération » a posteriori – est devenu largement dominant dans l'aire des « médias indépendants ». Or cette conception de l'information alternative montre, depuis quelque temps déjà, toutes ses limites, et est aujourd'hui en crise (5). En effet, le principe de l'*open publishing*, sans doute séduisant par son affirmation absolue du principe de liberté de publication, produit dans les faits de terribles confusions :

- Confusion entre les textes d'informations et les textes d'opinion ou d'humeur, qui sont finalement mis bout à bout sur un même plan ce qui finit par produire un effet de brouillage important.
- Confusion entre l'activité d'un collectif dont le champ d'action est la communication et l'information, et des contributions d'origine incontrôlable qui ne peuvent, à un moment ou un autre, qu'entrer en conflit avec le principe même d'une ligne rédactionnelle.
- Confusion entre la libre expression et le champ libre au « n'importe quoi », voir à l'instrumentalisation par n'importe qui (par exemple des infos postées par des groupes d'extrême droite).

C'est dans ce contexte qu'il faut placer les « dérapages » antisémites publiés sur certains sites d'Indymedia (dont Indymedia France), où le fait que chaque échéance de mobilisation y donne lieu à d'interminables polémiques groupusculaire au détriment de l'information réelle. C'est sans doute aussi les raisons pour lesquelles certains sites du réseau Indymedia (comme IndyACP à Madrid ou CEMAQ au Québec) séparent désormais les textes « proposés » des textes « publiés », en plus de s'être dotés d'une charte rédactionnelle explicite, comme la plupart des collectifs locaux d'Indymedia.
Mais au-delà des critiques que nous sommes nombreux à faire sur l'application du principe de l'*open publishing*, il faut aussi reconnaître que les projets fondés sur une dynamique de coopération entre des groupes et des individus – comme nous le pratiquons à samizdat.net – ne sont pas non plus sans révéler des limites, en particulier la difficulté des milieux militants à véritablement communiquer au-delà de leur cercle d'influence restreint, qui les conduit souvent aussi à privilégier la relation avec les médias *mainstream* et à sous estimer les réseaux de la communication alternative.

Pour un débat dans le mouvement

À partir de ces quelques remarques, et des diverses contributions sur le sujet qui ont circulé ces derniers mois (6), il nous semble important que s'ouvre une confrontation loin des polémiques et des procès d'intentions. Confrontation qui doit produire aussi de la coopération à brève échéance, pour ne pas en rester à un simple échange de point de vue. C'est de tout cela que nous entendons parler à la zelig. rc2 cette année, pas seulement entre « spécialistes », mais avec tous ceux et celles qui sont partie prenante des multiples formes de l'activisme politique et social aujourd'hui.

Samizdat.net

(1) Sur ces questions, voir le bilan de notre expérience à Gênes, à l'été 2001 : Jean-Pierre Masse, Aris Papathéodorou, *Communiquer à Gênes, communiquer Gênes*, sur samizdat. net :
http://infos.samizdat.net/article.php3?id_article = 163
(2) Hakim Bey, *Le credo médiatique fin de siècle*, disponible en français sur la Biblioweb de samizdat. net :
http://biblioweb.samizdat.net/article.php3?id_article = 12
(3) Hakim Bey, ibidem.
(4) Indymedia Théssalonique, *Lettre ouverte au réseau Indymedia*, juillet 2002. reproduit ci-dessus.
(5) Voir les éléments sur la crise d'Indymedia France sur le site web : http://france.indymedia.org.
(6) Voir en particulier Kandjare, *Les contre-sommets : traitements médiatiques et « spectacularisation » de la contestation*, sur samizdat. net :
http://infos.samizdat.net/article.php3?id_article = 161

Libre en fête. Du 21 au 23 mars 2002

Trois jours et deux nuits de dynamique festive pour la sauvegarde et la diffusion de la connaissance, pour la liberté d'expression, pour la reconnaissance des acteurs du libre, pour la reconnaissance de l'alternative. **Pourquoi une fête ?** Tros jours et deux nuits de découvertes et de rencontres autour du partage des connaissances, de la liberté d'expression, de la reconnaissance de l'alternative, et, en passant, pour rendre hommage à ceux qui sont dans l'ombre. (et pour le plan ! trois jours de teuf quand même) Ça commence quand ce projet ? c'est parti le 17 avril 2001, et c'est cette année du 21 au 23 mars 2003. **alors… ça se passe où ?** Ca va se passer partout ou on dispose de moyens pour réunir des gens, pour pouvoir faire une démo, pour parler, manger, mettre du son… Comme l'an dernier la première manifestation annoncée aura lieu en Bretagne dans une ferme de dégustation de produits… fermiers ;) **… et qui fait quoi ?** il y en a qui recherchent des lieux pour faire une animation, d'autres mettent en place le serveur web avec les logiciels adequats (gnu/linux debian, apache, php, mysql, perl, sympa, Spip,…). Il y en a d'autres qui attendent les annonces, et d'autres qui assurent internationalement la conception et le support des logiciels libres qu'on utilise. thanx. **Au fait, Libre en fête**, c'est sans doute un bon moyen de se faire connaître par chez soi tout en faisant parler du coin. Alors, rien n'empêche de proposer aux créateurs/mainteneurs/utilisateurs/documentalistes de logiciels libres de venir s'occuper des animations dans nos communes et expliquer comment utiliser un logiciel de traitement d'images, un générateur de sons, un lecteur dvd ? (mais faut pas l'dire fort ok ? ;^), un jeu en réseau, un navigateur web, un gestionnaire d'email […] et après la dégustation des produits locaux, on enchaîne sur une nocturne ? ; cool.

>> http://www.libre-en-fete.net

Sémantique politique de l'informatique libre

La révolution du libre est en marche depuis près d'une quinzaine d'années, et rien ne semble l'arrêter pour le moment. En partie grâce à Linux, le libre suscite l'intérêt des médias et des décideurs. Cet engouement n'est pas sans une tendance à dénaturer la philosophie du Libre Logiciel. C'est ce qu'amplifie, par exemple, l'utilisation abusive par la presse nationale du terme « logiciel *Open Source* » en lieu et place de « logiciel libre » (« *Free Software* »).

On peut comprendre que des anglophones utilisent le terme, pour lever l'ambiguïté de l'anglais sur le mot « free » qui veut d'abord dire libre, mais peut être interprété comme voulant dire gratuit, selon son usage vulgaire et commercial. Il n'y a pas de telle ambiguïté en français, et l'utilisation abusive d'un terme anglais non justifié ne fait que révéler une incompréhension du phénomène dont il est question, de sa philosophie, de sa culture, de ses enjeux. Ainsi, Richard M. Stallman est à l'origine du mouvement du logiciel libre et non pas de l'initiative *Open Source* ™. Querelle de clocher ? Non, importance de la sémantique du logiciel libre. Le mouvement du *Free Software* a été fondé en 1984. Le projet GNU fait partie de ce mouvement ainsi que le système d'exploitation GNU/Linux, souvent appelé « Linux », qui est en grande partie (mais pas totalement) issu du mouvement du Free Software. Ce mouvement véhicule des idées de liberté, de communauté et une certaine vision de société, à travers le logiciel libre. L'initiative *Open Source*, fondée en 1998, a pour objet, en partie, de favoriser l'accession des non-informaticiens au monde du logiciel libre, en mettant en avant les aspects utilitaires de ces logiciels, mais sans aborder l'esprit philosophique de cette communauté.

On ne doit pas attribuer au mouvement *Open Source* ce qui ne lui est pas dû. Les concepts *Free Software* et *Open Source* Software sont très proches, car ils décrivent techniquement les mêmes logiciels, mais diffèrent dans leurs buts et cette différence est essentielle. L'importance du mouvement du Free Software est capitale et irremplaçable, et le succès de GNU/Linux est avant tout le sien. A présent, l'existence du logiciel est reconnue internationalement et il est temps de revenir au fondement de ce mouvement : la liberté. En effet, ne vanter que les mérites techniques des logiciels libres en négligeant leur philosophie conduit à une impasse. L'enjeu réel du logiciel libre est avant tout social et politique. Si les logiciels libres suscitent aujourd'hui un intérêt technique à court terme, leur avantage technique n'est que la retombée, après quinze ans de combat, d'un modèle qui vaut surtout par ses effets à long terme. Ne voir que le court terme, c'est s'exposer continuellement à retomber dans les pièges du logiciel propriétaire, c'est ne pas apprendre. Le vrai moteur du Libre Logiciel est bien la Liberté, terme devant être pris dans le sens civique, politique, du terme : liberté d'expression, liberté d'association, liberté d'entreprise, liberté d'user à sa guise de l'information disponible et de la partager, au bénéfice de chacun, donc de tous.

De plus en plus de personnes peuvent utiliser les logiciels libres pour leur côté pratique, mais cela n'accroit pas pour autant la communauté du logiciel libre, et ne la pérennise pas. Nous ne bradons pas notre liberté pour de simples questions de commodité. Nous devons soutenir le logiciel libre pour ce qu'il est, même si le logiciel propriétaire devait s'avérer plus puissant ou plus efficace. Les questions de liberté et d'intérêt social sont au centre des préoccupations du monde du libre. Le mouvement du logiciel libre, se référant à l'utilité sociale, s'oppose à l'appropriation individuelle de la production intellectuelle dans le logiciel.

Profitant actuellement du succès des nouvelles technologies de l'information et de la communication, des groupes d'intérêt se mobilisent pour renforcer les droits de la propriété intellectuelle, au détriment de l'intérêt général qui veut que les connaissances soient un bien public universel, et également au détriment des droits fondamentaux que sont la liberté d'accès à l'information et la liberté d'expression. C'est oublier un peu vite que la motivation originelle et officielle de la propriété intellectuelle était et est toujours de préserver l'intérêt de l'humanité en reversant dans le domaine public une oeuvre qui survit ainsi à son créateur.

Finalement, le mouvement du logiciel libre prend racine dans un idéal qui postule la liberté absolue et le caractère universel du savoir et de l'information.

Frederic Couchet

Cyber-résistants du Libre

Pour beaucoup, le logiciel libre, fortement lié à l'Internet et à ses modes de communication associés n'est que le prémisse d'une cyber-révolution en marche. D'ailleurs, au vu d'évènements relativement récents (mobilisation de Seattle du 30 nov 99, succès d'Attac, etc.), on ne peut nier que les outils électroniques de communication prennent une place de plus en plus importante dans la mobilisation citoyenne. Le fantasme du cyber-résistant prend forme. On peut même rêver que, malgré le lobbying intense de grosses structures américaines et de spécialistes en propriété intellectuelle, le Parlement Européen ne procède pas à l'imminente modification de l'exception logicielle des paragraphes de la convention de Munich sur le brevetage. Pour autant, comme le rappelle Serge Halimi (1), les formes de mobilisation progressistes les plus efficaces et les plus démocratiques ne sont pas nécessairement les plus modernes. Il cite notamment parmi les écueils à éviter, celui de négliger l'impératif de l'organisation.

Nul ne peut nier qu'Internet, notamment par l'instauration de relations transversales entre individus, par l'accès rapide et facile à de l'information, par l'interconnexion globalisante des esprits humains, par la rapidité de circulation des communications est un lieu idéal pour l'action, mais l'action rapide, immédiate, vite organisée, vite oubliée. Pas l'action à long terme.

Souvenons-nous que le préfix « cyber » de l'expression cyberculture vient du grec cyber, dont l'éthymologie est partagée par les mots « gouverner » et « gouvernail ». Ainsi, on peut considérer la cyberculture comme une culture du gouvernail et du gouvernement. Le gouvernail étant la partie d'un bateau, d'un avion qui assure sa direction. La cyber-résistance, dont l'un des plus beaux fleurons, qui est aussi le seul produit réel de la cyberculture, est le logiciel libre ne peut se passer de gouvernail. Et un groupe d'individus communiquant principalement par des moyens électroniques doit tenir compte de règles de gouvernance, au risque sinon de ne rien produire du tout. Le cyber nous fournit un gouvernail, et Richard Stallman nous fournit sans doute un cap à suivre.

En effet, le succès du logiciel libre est principalement la conséquence d'une volonté, celle de Richard Stallman, qui a su matérialiser une idée révolutionnaire basée sur une réelle réflexion/vision politique à long terme. Le libre n'a pas été une révolution immédiate, mais plutôt un long changement de société. Richard Stallman lui-même conçoit le libre comme une révolution pratique et anti-utopique.

Ainsi, la réussite de Richard M. Stallman dans sa lutte vient de son habileté à éviter les écueils cités par Halimi. Au niveau des associations françaises, prenons l'exemple de l'APRIL à laquelle j'ai le bonheur de participer et dont la force est justement de tenir compte des limites de la cyber-résistance et de mettre en place une structure adequate. A bien y regarder, alors même que tenant compte du changement de mentalité où le militant est un incitateur d'action, participant à la définition de la stratégie politique et activiste globale, une association comme l'APRIL fonctionne principalement par le bon usage de l'intelligence distribuée, utilisant au mieux la capacité de chacun, distribuant les tâches, entraînant une mobilisation dans l'organisation (2).

Si on se base sur le nombre d'acteurs – et notamment les LUGS (3) –, on pourrait penser qu'il y a de nombreux militants prêts à agir pour leurs idées. Le problème est que la majorité d'entre eux se contentent d'aspects techniques et assimilent le débat d'idées à une vaine querelle. Les forts en gueule sont également légion, rois du verbiage, producteurs d'opinions et de sentences, mais plus rarement d'actions. L'activisme n'est pas seulement déterminé par la capacité à créer une liste de discussion (et encore). Ceux qui le pensent ne sont finalement que des « cyber-neuneus se taillant des pipes virtuelles » à longueur de journée.

Pour citer Philippe Quéau, à qui je dois la métaphore précédente du gouvernail : « La cyberculture est une culture de gouvernail et de gouverment : navigation et gouvernement de soi-même, gouvernement du collectif, gouvernement de personnes libres s'assemblant virtuellement sur la nouvelle agora du monde. » Le logiciel libre est l'expression la plus parfaite de cette agora, mais, pour autant, la résistance technique, politique et culturelle dans l'espace électronique a tout intérêt à tenir compte de l'expérience de l'activité militante traditionnelle. Scander « Linux, Linux, Linux » derrière son clavier ne fait pas de vous un cyber-résistant ou un hacktiviste.

Jérôme Dominguez

(1) Serge Halimi, Des « cyber-résistants » trop euphoriques, Le *Monde Diplomatique*, août 2000.

(2) Voir par exemple (sur le site de l'April) , l'opération Amazon : http://www.april.org/actions/brevets/

(3) LUGS : les groupes d'utilisateurs Linux - Note de la rédaction.

Légal

Numéro 1 – décembre 2002 - Prix : 0,5 euros.
zelig.rc2 le journal est publié par l'association samizdat.net pour le compte de l'équipe de la zelig. Directeur de la publication : Aris Papathéodorou. Imprimerie : Rivet (Limoges) – 05 55 047 49 50.
Dépot légal : 1er trimestre 2002 – Commission paritaire en cours.
Zelig c/o CICP - 21ter, rue Voltaire, 75011 Paris

Programme

Lundi 9 décembre

18h30-21h	✶ Internet alternatif pour les nuls	Les Vignoles
	✶ La crypto pour Macintosh	Les Vignoles
	❖ Palladium & TCPA	CICP
	❖ Cyberfeminist Open mic	CICP
21h30 à 00h	✷✷ After lalala : V. Hubert, Nodj, Unagi Inu, Cha-Cha-Cha-Laptop-Orchestra, Juicy Panic/Mami han+Norman Bambi, Sylvie + Guests éof - 15 ue Saint Fiacre 75002 Paris – M° Gds Boulevards – eof5@wanadoo.fr	

Mardi 10 décembre

18h30-21h	⌘ SPIP, système de publication sur l'Internet	CICP
	✶ Logiciels libres pour l'éducation – Installation serveur abuledu	CICP
	❖ Tout savoir sur le STIC	Les Vignoles

Mercredi 11 décembre

10h-18h	✶ Logiciels libres pour l'éducation – Démonstrations sur le réseau Abuledu	CICP
14h-16h	❖ Vidéosurveillance en France	CICP
14h-18h	✶ Gender Changer Academy – Les mains dans les machines	Les Vignoles
18h30-21h	❖ Les femmes font tourner les machines en ex-Yougoslavie et en Belgique	Les Vignoles
	✶ Logiciels libres de bureautique	Les Vignoles
	⌘ AlternC : outil pour hébergeurs	CICP

Jeudi 12 décembre

18h30-21h	❖ Wifi : les réseaux sans fil	CICP
	✶ Gender changer Academy – GNU/Linux pour les filles	Les Vignoles
	❖ Libre entreprise : réseau d'entreprises autour du libre	Les Vignoles
	✶ Gestion de mailing lists	CICP
	❖ Les hackers, la justice et les médias	CICP

Vendredi 13 décembre

18h30-21h	❖ Les dangers de l'extension de la propriété intellectuelle avec Alexandre Dulaunoy	CICP
	✶ Print, plug'n'politix : informatique et politique radicales	Les Vignoles
	❖ Mad Europe – Panorama des lois sécuritaires en Europe avec Tony Bunyan (Statewatch)	CICP
	✶ Firewall et réseau local associatif	Les Vignoles

Samedi 14 décembre

10-12h30	❖ Communication alternative : produire l'infos hors des médias	Les Vignoles
	✶ Crypto sous Windows	CICP
	✶ Crypto sous GNU/Linux	CICP
	⌘ Glasnost (logiciel de vote, et et partage d'informations)	Les Vignoles
	✶ Systèmes de fichiers cryptés sous GNU/Linux	CICP
14h-18h	❖ Suspects sous surveillance : retour sur quelques lois sécuritaires	CICP
16h-18h	❖ cybefeminism : revolution – Rencontre avec Cornelia Sollfrank	Les Vignoles
18h30-21h	✷✷ Yesmen	CICP
22h à ...	✷✷ After surprise	

Dimanche 15 décembre

14h-16h	❖ L'éthique du logiciel libre avec Loïc Dachary	CICP
14h-18h	✶ Sécurité réseaux : synsmurf, tunelling, etc.	CICP
	✶ Atelier Wifi : les réseaux sans fil	CICP
18h30	[Game over]	

⌘ DÉMOS ✶ ATELIERS ❖ DÉBATS/DISCUSSIONS ✷✷ FÊTES

Programme sous réserve de modification consulter le site web de la zelig.rc2 (http://www.zelig.org) pour confirmation.

« Ils ont des outils, que veulent-ils en faire contre nous, et que pouvons nous en faire contre eux ? »

Bruce Sterling

Qui ? Les gentils organisateurs

La zelig.rc2 est organisée par : Bugbrother, CNT-SII, Fédération informatique et libertés (FIL), Globenet, LSIjolie, Madchat Reposito, nettime-fr, pRiNT, Ras l'Front, samizdat.net, Les Virtualistes, Souriez vous êtes filmés, et des individu(e)s, monstres, mutant(e)s et cyborg...
Avec le soutien de : April (association pour la promotion et la recherche en informatique libre), l'Autre Net, Fédération anarchiste, Ouvaton, Observatoire du droit des usagers, Pl@cenet.
>> http://www.zelig.org/article.php3?id_article=19

Où ? Mais comment j'y vais ?

CICP – Centre international de cultures populaires
21 ter, rue Voltaire, 75011 Paris
Métro : Rue des Boulets ou Nation
Les Vignoles – Confédération nationale du travail
33, rue des Vignoles, 75020 Paris
Métro : Avron ou Buzenval
>> http://www.zelig.org/article.php3?id_article=22

Comment ? J'peux v'nir ?

L'entrée à l'ensemble des initiatives est *libre*. Pour les ateliers (✶) et les démos (⌘) pensez quand même à vous inscrire sur le web : c'est facultatif, mais cela nous aidera pour l'organisation).
>> http://www.zelig.org/inscriptions.php3

Quilombo. De la matière pour l'esprit

La boutique-librairie Quilombo est un lieu de diffusion, d'information et d'échanges. Une librairie avec des ouvrages et des publications sur les luttes sociales, les mouvements, l'antifascisme, le féminisme... Une librairie où l'on privillégie les petits éditeurs engagés et passionnés... Une boutique avec vêtements (tee-shirts, sweat-shirts), des affiches, des autocollants, badges, patchs, etc. Pendant toute la durée de la zelig.rc2 la boutique-librairie Quilombo sera ouverte aussi pour diffuser de la contre-culture digitale...
>> 23 rue Voltaire, 75011 Paris.
Tél /fax 01 43 71 21 07 – quilombo@wanadoo.fr

Libres ! Logitiels pour Windows et Mac OS X

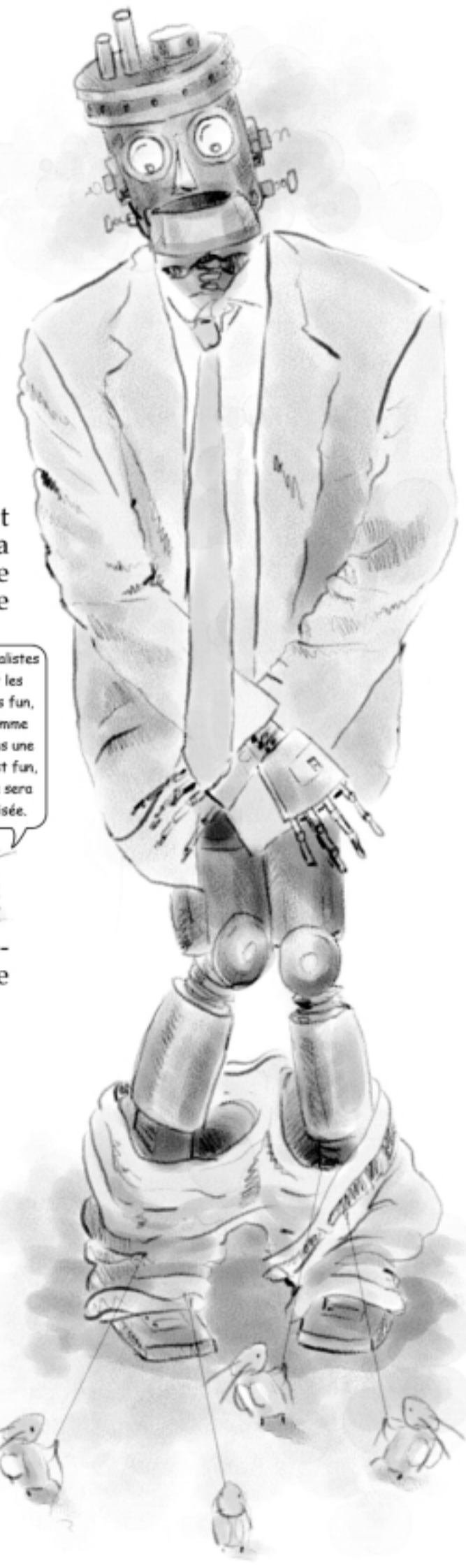
Peur d'installer un système libre GNU/Linux ou *BSD sur votre ordinateur ? Contraint par le salariat à travailler sur un système propriétaire du genre Windows ou Mac OS X ? Nous avons préparé une compilation de logiciels libres (sur CD-Rom) pour remplacer Internet Explorer, Microsoft Word, Outlook et autres Entourages, qui permettra à chacun et chacune de découvrir ces logiciels développés de façon coopérative, librement utilisables et modifiables (si nécessaires). Sur le CD-Rom sont aussi présentes des informations sur le logiciel libre en général, de sera diffusé à un prix modique le week-en du 14-15 décembre.

E M B A R R A S T A C T I Q U E

COMMENT ÇA MARCHE

Pour bien contrôler une machine, il faut en connaître les entrailles.

On peut en dire autant pour ces individus et entreprises dont l'objectif est d'être toujours plus riches, quelles qu'en soient les conséquences : en démontant ces puissances, on peut dévoiler leurs méthodes. Ainsi, chacun peut voir leur façon d'agir et imaginer comment les contrôler. Nous appelons cette technique *l'embarras tactique*.



En un mot :

Choisis bien ta cible et cherche ce qui pourrait la déséquilibrer—quelque chose de très fun, de préférence.

Comment faire? Imagine ta cible en train de déraper totalement. Qu'est-ce qui pourrait le rendre aussi fou ?

Profite de cette réaction. Ecris un communiqué de presse et envoie-le par e-mail à des centaines de journalistes.

Préparation du communiqué

Imagine un article "objectif" sur l'événement. De quoi aurait-il l'air ? Sois réaliste. Puis, écris cet article. (Des scrupules ? Ce n'est qu'un grand classique des transnationales pour vendre produits et candidats.)

A la pêche aux menaces

Le plus simple moyen d'embarrasser quelqu'un de puissant est de montrer à quel point il est mesquin. Apprends à savourer les menaces de procès et à t'en servir au tribunal de l'opinion publique.

Exemples historiques d'embarras tactique :

En 1967, des Yippies jetèrent du balcon de la Bourse de New York cent billets d'un dollar. Les journalistes qu'ils avaient conviés à leur action racontèrent au monde entier comment les courtiers, dévorés par l'appât du gain, lâchent tout et se ruent sur les billets comme des fous.

Coût de l'action : $100. Perte boursière suite à la clôture : des millions de dollars—sans parler de l'image.

http://gatt.org/yippies

* La réponse de Bush lors de conférence télévisée, juin 2000.

Au cours de la campagne présidentielle de Bush, ®™ark mit en ligne GWBush.com, qui ressemblait exactement au site officiel du candidat, mais qui se moquait de Bush et critiquait le financement privé de la campagne électorale. Lorsque Bush découvrit le site, il devint furieux et fit des déclarations on ne peut plus stupides à la télé.

®™ark envoya un communiqué de presse par e-mail à des milliers de journalistes. La couverture médiatique fut telle que l'équipe de Bush dut arrêter la procédure judiciaire qu'elle avait intentée, et retirer ses plaintes.

Coût pour ®™ark : $0. Bush se révéla pleurnichard et capable d'incroyable bassesse.

http://rtmark.com/bush

Afin de contrer l'«abandon planifié» par la municipalité d'un historique quartier ouvrier de Séville—un plan dont le but était d'en expulser les habitants, afin d'augmenter la valeur du quartier—des activistes mirent des centaines de logos officiels légèrement détournés sur les crottes de chien qui parsemaient le voisinage. Les délégués d'une conférence internationale sur l'urbanisme ne purent que s'étonner du fait que Séville sponsorisait de la merde.

LOGO DE LA VILLE

"No me ha dejado." Vous ne m'avez jamais abandonné.

LOGO ALTÉRÉ

"Sí me ha dejado." Vous m'avez abandonné.

Coût pour les chiens : minime. Peu après, les services sanitaires recommencèrent enfin à fonctionner. Plus important, l'opération immobilière apparut au grand jour, et devint l'objet d'une lutte commune.

http://www.sindominio.net/fianbrera