INFORMATIQUE ET SECURITE

On a beaucoup parlé, récemment, de Sécurité et d'Informatique, de sécurité de l'informatique à propos des attentas qui ont affecté au printemps 1980 les installations d'ordinateurs de Philips et de C.I.I. Honeywell-bull.

Ces attentats n'ont fait que jeter une lumière plus crue sur une notion déjà à l'honneur depuis longtemps dans les milieux spécialisés qui apparait comme étroitement liée à l'Informatique à savoir la Sécurité.

En effet, ce n'est pas aujourd'hui que l'on se soucie de protéger les installations informatiques contre les dangers naturels ou humains ou que l'on utilise des machines programmables et à mémoire pour protéger des biens et des personnes.

Ce n'est pas d'aujourd'hui non plus que l'on se préoccupe de tirer avantage (économique, idéologique, etc.) de la protection de l'informatique ou par l'informatique.

Ces quelques considérations nous conduisent à traiter la question de l'Informatique et Sécurité de la façon suivante :

- La protection des systèmes informatiques
- L'informatique comme outil de protection
- Le profit tiré du couple informatique-Sécurité.

Gare à la fraude

Tout d'abord on a songé à protéger les installations contre les risques naturels : incendie, dégats des eaux, excès de chaleur ou de froid, trop forte intensité des champs magnétiques, etc.

On se prémunit contre ces dangers au moyen d'une ignifugation des salles d'ordinateurs, d'une climatisation, d'une bonne isolation des équipements électriques...

On veille à stocker les archives (bandes ou disques magnétiques) en des lieux bien protégés et bien séparés, à dupliquer les fichiers et à ne pas conserver toutes les copies en un même endroit.

De même il faut pouvoir parer les pannes de matériel : prévoir des machines de secours, une alimentation électrique de remplacement, doubler, tripler les lignes de transmission...

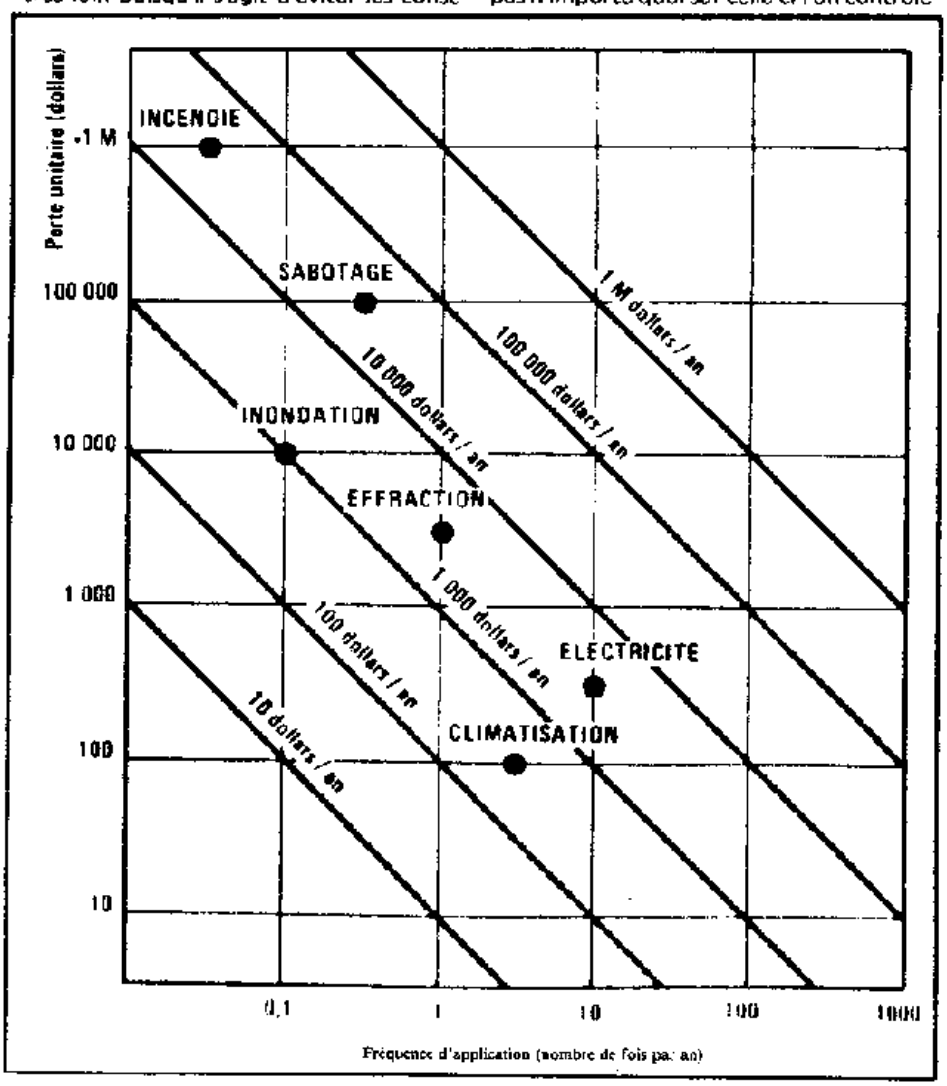
Enfin, comme disent les informaticiens, le principal danger c'est l'homme. Des mesures de sécurité sont prises contre les erreurs de manipulation ou de programmation, les vols (de matériel, de temps-machine, de programmes).

On a parlé d'escroqueries et de fraudes, spectaculaires par leurs effets car elle portent sur des sommes considérables, réalisées par des informaticiens astucieux. On imagine même que la part de fraude non détectée est très importante, bien supérieure peut être à celle qui est découverte. Ainsi 10 % seulement des délits informatiques seraient recensés selon les experts d'après une information rapportée par *Informatique et Gestion* (N° 109, oct. 1979).

Le souci de protéger les installations va très loin puisqu'il s'agit d'éviter les conséquences d'actes de destruction, de sabotage, d'attentats, de grèves bien sûr et même de guerre. La presse s'est faite l'écho des attentats commis au printemps dernier. Le courrier d'un lecteur de *Libération* évoque différente formes de sabotage. Le rapport d'une commission Suédoise (SARK) cite les risques de grève, d'attentat ou de guerre.

Bunker informatique

L'imagination n'est pas défaillante lorsqu'il s'agit pour les détenteurs d'ordinateurs de lutter contre les « risques humains ». En général, on ne pénètre pas comme on veut dans une salle d'ordinateur. Souvent il faut introduire un badge dans un appareil pour déclancher l'ouverture de la porte de la salle-machine. Des systèmes de surveillance des salles, des circuits de télévision, de gardiennage sont également utilisés. N'importe qui n'a pas accès aux machines ! N'importe qui ne fait pas n'importe quoi sur celle-ci ! Un contrôle



est exercé sur l'activité des différentes catégories de personnel qui travaillent sur le matériel ; une réglementation stricte de leurs tâches est souvent édictée.

Pour programmer sur une machine et plus encore pour mettre à jour un fichier il faut fréquemment utiliser des mots de passe. Des procédures sophistiquées sont employées pour vérifier l'identité des utilisateurs (on leur demande par exemple d'indiquer les dates de naissances de leurs enfants et on compare leurs réponses à celles qui ont été préalablement enregistrées).

On a recours au cryptage des informations, c'est-à-dire à leur chiffrement de telle sorte que leur sens initial soit caché. Des systèmes de verrous et de clefs d'accès peuvent également être mis en place. Une grande attention est aussi portée à la destruction des documents périmés ou erronés qui pourraient être récupérés par des concurrents, les syndicats, voire des espions de même qu'on contrôle la destination des documents et qu'on vérifie le bien fondé des raisons avancées par les divers destinataires de les recevoir.

Dernier aspect de la protection de l'informatique : la protection des informations confidentielles. Les fichiers informatisés constituent, on le sait, des moyens de conservation, de regroupement, de confrontation de renseignements multiples sur la vie privée des personnes ou de données confidentielles (procédés de fabrication, secrets bancaires, militaires ou policiers).

La protection de ces fichiers est à la fois une question de sécurité pour les personnes ou les organismes qui détiennent les informations et pour ceux sur lesquels portent les renseignements conservés. La Sécurité est alors présentée comme moyen de sauvegarder les libertés (vie privée, avantages collectifs...) !

Je badge, tu badges, ils badgent...

Des ordinateurs ou des microprocesseurs sont utilisés fréquemment comme instruments de surveillance ou de détection. Le Centre Beaubourg est une bonne illustration de cette utilisation de l'informatique. 6000 informations sont prises en compte dont 4200 proviennent de signalisations et alarmes issues de divers capteurs (détecteurs d'incendie, contacts d'ouverture de portes et de positions d'ascenceurs, capteurs volumétriques sensibles aux déplacements de personnes). Toutes ces informations sur les dangers naturels ou les comportements des gens (vols par exemple) sont analysées par un ordinateur auquel sont branchés des écrans de télévision. D'un poste central on observe donc la vie du Centre en permanence et on peut prendre des décisions très rapidement.

L'utilisation des badges pour réglementer l'accès aux salles-machines peut être étendue à la surveillance des allées et venues du personnel dans certaines entreprises.

Et à partir d'un certain degré d'équipement en caméras ou en appareils à badger il devient intéressant de confier l'analyse des informations produites par ces dispositifs à l'informatique.

La protection des locaux se développe. Ainsi pour le Palais des Festivals de Cannes a-t-on prévu un ordinateur qui contrôle que toutes les lumières sont allumées, qui reçoit les signaux des détecteurs d'incendie ou d'alarme, qui vérifie par exemple que si la porte A est ouverte, la porte B est bien fermée comme il se doit etc.

Toujours à Cannes on envisage l'implantation d'un autre ordinateur pour le traitement des statistiques ayant trait aux incidents qui peuvent se déclarer dans un édifice de ce genre afin de pouvoir y porter remède.

Les coffres-forts des entreprises — des banques en particulier — sont également équipés de systèmes d'alarme, d'appareils électroniques de détection reliés à la Police ou plus récemment à des centres de surveillance.

Télé-alarme

La commercialisation du Vigiphone est réalisée. Il s'agit d'un appareil composé de microprocesseurs qui fonctionne comme système de surveillance et de transmission d'alarme grâce à un branchement sur le réseau téléphonique habituel. Les incidents sont signalés de façon codée à un poste de surveillance lequel peut alors identifier l'origine de l'alarme. C'est un appareil recommandé par ses fabricants pour la protection des résidences principales et secondaires, des locaux industriels ou commerciaux, des lieux publics fermés ou... pour la détection de la pollution. Il est même conseillé aux personnes âgées ou handicapées. Cela rejoint les préoccupations du Ministère de la Santé dont l'un des objectifs à moyen terme vise au développement des systèmes de surveillance ou de télé-alarme des personnes âgées.

Le P.D.G. d'une société installé en Belgique a même fait installer une « maison informatisée » où à côté de la régulation des activités ménagères (cuisine, appareils électro-ménagers,...) on trouve des systèmes de surveillance extérieurs (des abords de la maison) où intérieurs (surveillance des enfants, déplacements de malfaiteurs éventuels...). A côté de cette maison à l'équipement bien sophistiqué on songe à des systèmes plus modestes pour H.L.M. par exemple. Pourquoi ne pas envisager, comme le suggère *Remue Ménage*, l'idée du balayage électronique des entrées d'immeubles : seuls les habitants munis de leurs numéros pourraient franchir la porte d'entrée, à la rigueur un parent ou un ami doté pour la circonstance d'un numéro de visiteur utilisable une seule fois ? Pourquoi ne pas y ajouter d'ailleurs quelques caméras et écrans de contrôle pour la détection des rôdeurs ou des maraudeurs !

Autre domaines d'application de l'informatique : la Sécurité des moyens de paiement. On connaît déjà les cartes de crédit à micro-processeurs créées par certains réseaux financiers tels Eurochèques ou les Caisses d'Epargne lesquels ont institué la carte de garantie, carte de haute sécurité avec photo infalsifiable qui rend difficile l'utilisation de chèques volés. On connaîtra peut-être les terminaux à domicile permettant des achats sans quitter son chez-soi après avoir tâté de toutes les formes de « monaies électroniques » et de « terminaux points de vente ». IBM vient bien de concevoir un système électronique de vérification des signatures !

Le contrôle social s'insinue

Il faut parler aussi de la sécurité informatique liée au fichage. Police, armée utilisent des fichiers informatisés. Les Pouvoirs Publics Allemands dans la chasse aux terroristes, l'administration britannique dans sa lutte contre l'I.R.A font appel à des matériels et programmes informatiques perfectionnés. La carte des données personnelles C.P.8 imaginée par C.I.I. Honeywell-Bull (dont parle le C.I.I.I. par ailleurs) s'ajoutera bientôt peut être à la carte d'identité infalsifiable conçue par le Ministère de l'Intérieur.

L'informatique sert déjà à assurer le vol en commande automatique des avions, à faire démarrer où s'arrêter les métros, à rendre régulière la circulatin routière, tout ceci pour notre sécurité... Demain ce sera la reconnaissance de la voix, des empreintes digitales, du poids des personnes.

Le contrôle social s'insinue. Ainsi s'il n'avait pas achoppé sur des difficultés techniques le projet d'une directrice de procéder par un système informatique à l'inscription des enfants en maternelle en édictant des règles uniques applicables partout (de priorité notamment), en obligeant les parents à déclarer leurs adresses et changements de domicile éventuels n'aurait il pas vu le jour ?

Les profits de la sécurité

La sécurité est une affaire lucrative. Les équipements et les contrôles par programmes pour assurer la protection des installations informatisées coûtent très cher. En plus, on surdimensionne volontiers les configurations, on double ou triple les lignes de transmissions pour éviter d'être bloqué par des pannes ou des incidents... De même les ordinateurs qui assurent la protection des gens ou des biens sont à des prix élevés.

Evidemment de multiples firmes vendeuses d'équipements ou de conseils fleurissent sur le marché de la sécurité. Les retombées rémunératrices bénéficient aussi aux compagnies d'assurance. Des entreprises réalisent des économies en achetant des micro-processeurs qui, par exemple, peuvent détecter des dangers humains ou naturel.

On ajoutera les organismes qui vendent de la formation à la sécurité. C'est ainsi qu'après les attentats de Toulouse on a vu surgir en nombre inhabituel des publicités proposant des « solutions anti-fraudes » ou certifiant pouvoir assurer « à des prix très compétitifs » les traitements automatiques pour le compte des victimes de la destruction de leurs centres informatiques.

Parmi les bénéficiaires de l'évolution des technologies de protection par l'informatique aussi bien que par la publicité faite sur les quelques attentats se trouvent au premier plan les officines de sécurité. Celles-ci sont maintenant dotées de moyens électroniques nouveaux remplaçant ou complétant élégamment les chiens et vigiles musclés. La peur du sabotage ou de la destruction — non limitée d'ailleurs au domaine informatique — leur donne un coup de fouet et l'on voit le nombre de ces agences, leurs effectifs et leurs chiffres d'affaires se multiplier.

Une association, le C.O.R.S.I.A (Comité de Recherche pour la Sécurité des Systèmes d'Information Automatisés) a même vu le jour. Elle est présidée par Vitalis Cros, un préfet honoraire. Elle n'a bien sûr pas de but lucratif mais elle met en évidence le profit non pécuniaire que l'on peut recueillir de la sécurité.

En effet, si un profit économique considérable est retiré de la sécurité informatique il convient de ne pas négliger le bénéfice idéologique au sens large que l'on espère gagner grâce au discours sur la sécurité développé par les individus et organismes dont le C.O.R.S.I.A fait partie.

A nouveaux maux, nouveau mot : la sécuritique !

Un terme a même été inventé, la sécuriti-

que qui se définit comme l'ensemble des techniques d'analyse, de transmission et de gestion des informations de sécurité.

A première vue, protéger les machines n'est pas un souci contestable. Pourtant les mesures prises : contrôles d'accès aux salles-ordinateurs, aux fichiers ; élaboration de mots de passe pour accéder aux informations, aux traitements ; réservation des transactions à certaines personnes sont autant de moyens d'habituer les travailleurs aux contraintes, aux contrôles, à la surveillance, à la hiérarchie.

Ces mesures créent un état d'esprit ou l'entretiennent. Ainsi C.I.I Honeywell-Bull profite de pseudos attentats contre son établissement de Louveciennes, montés en épingle par le *Matin*, afin de procéder à un renforcement — bien réel celui-ci — du contrôle des allées et venues du personnel.

La protection du dispositif informatique d'une organisation, d'une entreprise peut être entendue au sens large. Les mesures prises pour assurer la sauvegarde des informations et de leurs supports peuvent amener à restreindre la circulation des personnels non directement liés à l'informatique, à renforcer les contraintes de transmission, de communication, de conservation de documents à bien d'autres personnels que les informaticiens. L'informatique peut fournir l'occasion de prendre des décisions visant en fait à freiner les luttes ou revendications des salariés. De même en tant que secteur névralgique elle peut servir à justifier les limitations du droit de grève pour les travailleurs touchant à l'informatique.

Ne négligeons pas non plus l'aura « machine infaillible » qui enveloppe l'ordinateur. Avec plus ou moins de nuances on entend dire que la machine ne se « trompe pas » à partir du moment où elle est convenablement servie. Quelle sécurité pour les utilisateurs par rapport aux « traitements manuels si peu fiables » ! Quelle idée force pour faire taire les esprits dubitatifs devant sa majesté l'informatique !

Une société plus vulnérable ?

Contrôler ne suffit pas ? Alors on cherche à faire intégrer par les travailleurs liés à l'informatique les normes de sécurité que l'on définit. Ainsi naît l'idée d'une « déontologie du personnel informatique » que l'on trouve par exemple dans le dossier Sécurité élaboré par le C.X.P (Centre d'Expérimentation de Progiciels).

Dans le même débat qui prend corps autour de l'alternative centralisation/décentralisation ce dernier terme peut recouvrir un renforcement de la sécurité plutôt qu'une meilleure répartition du pouvoir de décision.

« L'ordinateur central » a été largement présenté par la presse au lendemain des attentats récents comme un «colosse aux pieds d'argile ». Neutraliser un gros ordinateur par la grève, le sabotage, la destruction ou simplement le freinage c'est quelquefois pouvoir bloquer l'activité d'une entreprise ou d'une administration. La déconcentration de l'informatique dans le secteur bancaire s'est accélérée après les grandes grèves de 1974. Dans son projet de carte d'identité informatisée, le Ministère de l'Intérieur prend bien soin de répartir les informations et leur traitement entre plusieurs mini-ordinateurs reliés par un réseau de communication plutôt que de tout rassembler sur un ordinateur central, unique.

L'éparpillement des ressources informatiques apparaît également comme un remède possible à la « vulnérabilité d'une société informatisée » expression employée dans le rapport du groupe d'étude suédois SARK qui recense tous les risques (des défaillances humaines à l'espionnage et aux actes de guerre) que court une société largement pénétrée par l'informatique.

En matière de sécurité, comme dans bien d'autres domaines, on préfère agir sur les

conséquences des phénomènes en renforçant les protections que de s'attaquer aux causes en recherchant vraiment pourquoi l'informatique est perçue par bien des individus et des organisations comme un danger.

Quand il s'agit de comprendre ou de réprimer, une bonne partie de la presse choisit la répression des attentats ou des sabotages au lieu de chercher à comprendre les raisons de ces actes.

Sécurité et (liberté)

Deux autres mots sont également associés de manière caractéristique : Sécurité et Liberté.

On sait que ces deux mots sont chargés de caractériser une loi passablement répressive qui vient d'être votée par le Parlement. On connait l'essor des réactions symptomatiques telles que le développement des agences de sécurité-gardiennage ou du mouvement légitime défense. Pourtant on ne fait pas toujours le lien entre l'informatique et les termes associés Sécurité et Liberté. Et même des idées d'apparence libérale qui ont cours dans le domaine de l'informatique peuvent se révéler redoutables.

D'aucuns ont bien compris et/ou souligné le parti qu'on pouvait tirer d'une mesure libérale comme la création de la Commission Nationale Informatique et Libertés (CNIL) en matière de sécurité.

Il suffit en effet à celui qui met en œuvre un système informatique d'obtenir l'aval de la CNIL pour avoir les coudées franches. Cette commission d'une certaine manière rassure, sécurise les réalisateurs d'applications qui, une fois le label de « non nocivité pour les libertés » décerné par elle, sont à l'abri de toute critique. Ce rôle de la loi informatique et liberté et de la CNIL est par ailleurs analysé par le C.I.I.I de façon plus détaillée.

En temps de crise de société enfin, l'informatique apparaît comme un moyen de rassurer. On peut tout d'abord lui donner une couleur sociale. Ce seront les systèmes de télé-alarmes ou de télésurveillance pour les personnes âgées vus plus haut. Grâce à ces appareils les vieillards seront secourus s'ils sont victimes d'une défaillance ou d'une agression mais par la l'isolement bien connu du 3e âge se trouvera renforcé. En toute bonne conscience la sécurité matérielle des personnes âgées étant assurée par ces nouvelles technologies on pourra se dispenser de développer une politique de (réi)insertion de ces dernières dans la cité, une politique qui alors ne viserait plus que le confort moral, affectif, social des vieux.

La serrure électronique

Par ailleurs, les machines qui servent au travail à domicile, à passer des commandes auprès des fournisseurs, à recevoir des informations, à se distraire etc. sans sortir de son domicile sont présentées, entre autres arguments, comme des remèdes à « l'insécurité grandissante qui règne dans nos villes impersonnelles ». On peut y ajouter une campagne de revalorisation de la cellule familiale et du domicile jointe à un processus de normalisation excluant les personnes « sans domicile fixe » ou les « déviants » par rapport au mode de vie familial type.

La sécurité survient parfois où on ne l'attend pas. Un numéro de *Sciences et Vie* d'octobre 1980 décrit un concours sur les ordinateurs personnels réservés aux adeptes du micro-ordinateur dans lequel est primée la réalisation « d'une serrure électronique à clé ». Cette serrure peut commander à tout un équipement électrique (gache de porte, coffre-fort, voiture, etc.). A partir de cette réalisation, est il ajouté, grâce à un circuit imprimé enfichable, on pourra aisément mettre en place un système de passe à plusieurs niveaux pour hôtels, bureaux, etc.

Arrivés à ce point du texte nous n'avons décrit que les équipement de sécurité qui existent ou dont la réalisation est proche de même que nous n'avons rapporté que le discours de sécurité tel qu'il est le plus largement répandu sans verser dans la science fiction ou l'anticipation.

Et dans 20 ans

Essayons maintenant d'imaginer la vie quotidienne telle qu'elle pourrait être dans 20 ans (1).

Demain les terminaux à réponse vocale existeront. Les isolés, les inquiets pourront dialoguer véritablement avec des machines. Demain les maisons pourront être de véritables forteresses — comme le disent déjà des publicités — protégées de l'extérieur par des appareils de détection, de surveillance dont les signaux seront analysés par l'ordinateur qui se chargera de déclancher les ripostes efficaces (signal d'alarme ou pièges à feu ?). Ces châteaux-forts » (dit toujours la publicité) seront aussi équipés de procédés de contrôle interne : surveillance des enfants à distance, du tirage du chauffage ou de la cuisinière à gaz, etc.

Demain encore grâce aux dispositifs précédemment décrits et à ceux qui restent à inventer on aura moins besoin de « s'aventurer » dans les villes décrites comme peu sûres où de toute façon d'autres systèmes contrôleront les déplacements des gens suspects par définition (les honnêtes gens étant chez eux !).

Dans « *L'ordre cannibale* » J. Attali parle d'un neurologue américain nommé Delgado qui suggère d'auto surveiller le comportement d'individus jugés prédestinés à la déviance, en implantant des microprocesseurs de type C.D.S., dans la zone frontale de leurs cerveaux afin de surveiller à distance leur agressivité et de libérer automatiquement un calmant si nécessaire.

Bien sûr le personnage est réputé, paraît-il, pour ses idées ultra-réactionnaires. Ses opinions sont encore discutées. Pourtant si l'on n'y prend pas garde insensiblement grâce aux techniciens ou brutalement à cause de ce genre d'idéologues un monde rappelant celui décrit par G. Orwell dans 1984 peut, à brève échéance, s'épanouir.

Commission Vie quotidienne et Contrôle social.

(1) Inconvénient de ce type d'extrapolation, c'est qu'elle ne tient compte que des tendances actuelles, et évacue les effets des contres-tendances : résistance à l'informatisation, luttes sociales sur le terrain des libertés, changements politiques... Il n'en reste pas moins que la dynamique d'une informatisation tous azimuts conduit à de nouvelles formes de totalitarisme qui trouvent un terrain favorable dans la politique giscardienne.

DOCUMENT

Ce document du ministère du Travail n'est pas récent mais garde toute son actualité. Il illustre l'évolution des conditions de travail des personnels de gros centres informatique, soumis à des contraintes exorbitantes du droit commun et de même nature que celles qui existent dans les centrales nucléaires. Les grands centres y apparaissent comme des *quartiers de sécurité renforcée* : les travailleurs sont recrutés sur tests psychologiques, enquêtes policière et auprès des anciens employés ; ils sont surveillés en permanence et soumis à la délation ; ils y vivent à l'écart des villes, derrière des clotures électrifiées, gardées et cloisonnées ; ils travaillent en continu dans des équipes variant en permanence... Que restera-t-il des relations sociales, des libertés, des droits syndicaux ? Pas grand chose si on laisse cela s'implanter...

3. LA PREVENTION

3.1 Mesures préventives concernant les personnes.

Les personnels peuvent être, en matière de sécurité, considérés sous deux aspects : d'une part en tant que victimes potentiellement capables ou non de se protéger par elles-mêmes, soit au contraire en *tant qu'agents responsables d'un risque.*

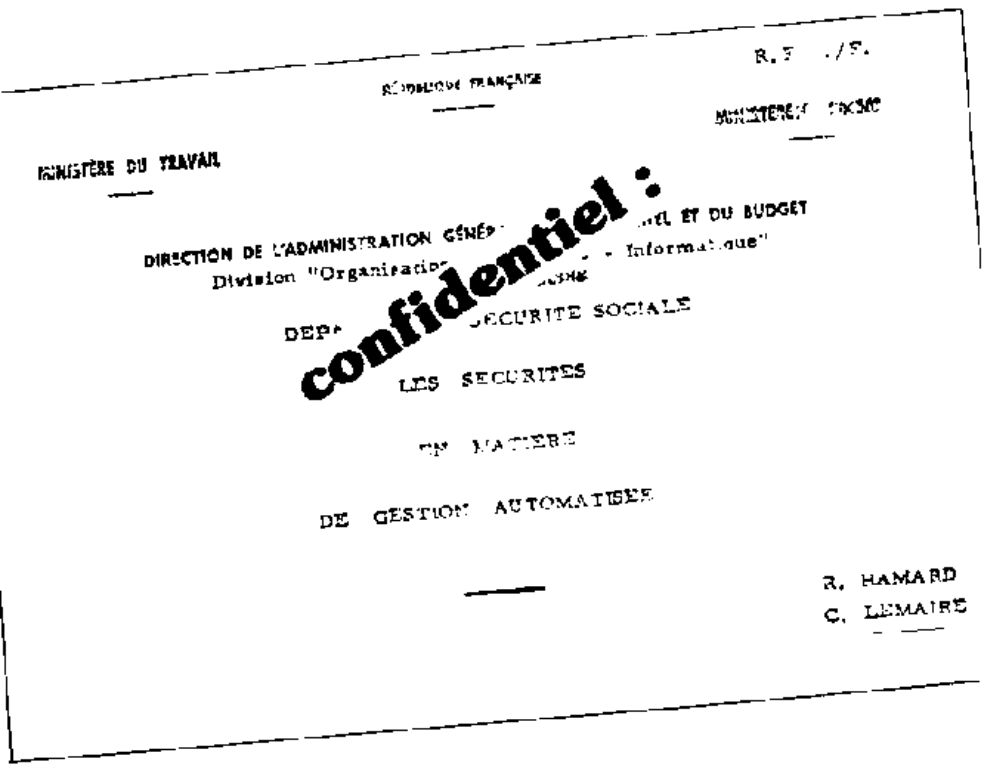
(...)

3122. Risques d'origine volontaire.

Nou verrons qu'on peut prévenir les malveillances d'origine extérieure par une bonne organisation du contrôle des accès. *Il est plus difficile de prévenir les malveillances de personnels internes.*

Tout au plus *cherchera-t-on à éviter d'employer à l'exécution des travaux informatiques toutes personne détectée ou connue comme caractérielle, pronant la violence et susceptible de vengeance ou de sabotage, de même que tout agent congédié ou démissionnaire dans de mauvaises conditions.*

De toutes façons, il convient de toujours *travailler à l'oide d'équipes dont on fera si possible varier la composition.* Personne en particulier ne doit être admis à travailler seul dans des locaux ou sur des fichiers de classe 1 ou 2. Toute duplication du fichier de



R.T ./S.

RÉPUBLIQUE FRANÇAISE

MINISTÈRE DU TRAVAIL

DIRECTION DE L'ADMINISTRATION GÉNÉ... ...EL ET DU BUDGET
Division "Organisation ... - Informatique"

DEP... ...SECURITE SOCIALE

confidentiel :

LES SECURITES

EN MATIERE

DE GESTION AUTOMATISEE

R. HAMARD
C. LEMAIRE

classe 1 ou 2 hors exploitation normale, doit faire l'objet d'une demande écrite suivie de l'autorisation du responsable de l'exploitation. Le responsable des archives exercera un contrôle quotidien sur la présence, notamment en bandothèques, des fichiers qui lui sont confiés. En outre le responsable de l'exploitation contrôlera que tout nouveau programme modifié n'aura pas eu d'incidences anormales sur les fichiers en cause.

Enfin et surtout, il faut savoir que *des contrôles tant systématiques que par sondages sont effectués et que toute disposition étant prise pour identifier l'auteur d'une malveillance, celui-ci encoura une sanction particulièrement sévère pouvant aller jusqu'au licenciement pour faute lourde.*

(...)

32. Mesures préventives concernant les bâtiments.

321. Implantation des locaux.

L'implantation du centre doit être choisie de façon que son environnement comporte le minimum de risques de dommage. A ce titre, un certain nombre de règles doivent être autant que possible respectées :

— éviter la proximité des centres urbains : cette décentralisation permise de plus en plus par le télétraitement qui unit le centre à l'établissement géré, évite de nombreuses causes de dommages (voisins à fort risques d'incendies...)

Elle améliore en outre la fidélité des personnels qui, résidant à proximité d'un centre isolé, sont moins aisément tentés par la concurrence.

(...)

323. Organisation des accès.

Une insuffisance du contrôle des accès aux locaux facilite les malveillances physiques et les détournements divers des informations. La sécurité des matériels et des informations commence par une réglementation des accès.

3231. Contrôle des accès extérieurs.

Dans le cas d'un bâtiment consacré exclusivement au centre informatique, *l'existence d'une clôture éventuellement électrifiée sera une première protection.*

Un poste de gardiennage peut être installé, mais ne sera efficace que dans la mesure où des consignes précises règlementeront les accès. Ces consignes impliquent généralement la définition d'autorisations d'accès individuelles et leur contrôle strict au moyen de

— listes nominatives ;

cartes ou badges magnétiques renouvelables périodiquement.

Le gardien tiendra en outre un registre nominatif des entrées et sorties avec mention horaire précise (heure et minute) de passage.

3232. Contrôle de la circulation dans le centre.

Les mesures applicables commencent par l'étude de la disposition des lieux en fonction des priorités de protection liée aux classes de locaux.

Si toute personne autorisée à pénétrer dans le centre aura par définition accès aux locaux de classe 3, on se trouvera bien *d'établir un barrage supplémentaire au niveau de l'accès aux locaux de la classe 2, l'autre pour l'accès de la classe 1, avec des restrictions croissantes d'autorisations.*

(...)

Il existe notamment des systèmes de contrôle qui peuvent comporter des dispositifs d'alarme et qui se déclenchent lorsqu'une personne tente de s'introduire dans un local où elle n'est pas autorisée à se rendre, avec verrouillage automatique des issues.

En outre, dans des centres importants, *des systèmes très sophistiqués peuvent permettre une surveillance automatique par ordinateur* (ordinateur de contrôle de processus) ou par un central téléphonique programmable, exerçant ainsi une véritable gestion des accès.

A noter que les visiteurs ne doivent sauf exception, jamais être admis en classe 1 ou 2.

415. Détentions des malveillances

(...)

Il convient en réalité de se protéger de l'intérieur du centre. Déjà, l'accès aux locaux où sont archivées les données confidentielles doit-il être sérieusement protégé. Mais surtout, *le responsable des archives et de la bandothèque, recruté entre autres qualités pour sa parfaite intégrité, aura pu coder préventivement l'étiquetage de ses fichiers et exercera une surveillance constante de la présence et du classement correct des divers supports qui lui auront été confiés.* Un autre mode de détection est indispensable, par l'examen quotidien des temps-machines au regard des volumes traités ou décomptés. A ce propos également, nous noterons combien la généralisation des comptages s'avère utile. Les éditions de documents seront surveillées tant au niveau de l'imprimante qu'à celui de la sortie du Centre. De même pour la destruction de documents officiels.

Par ailleurs, *tout comportement anormal de la part d'un ou plusieurs membres des personnels du Centre pourra motiver une enquête discrète de la part des responsables et une surveillance renforcée de leurs possibilités d'action.*

Enfin, et *surtout, rien n'interdit aux responsables du Centre de faire preuve de la plus large imagination et d'utiliser des procédés de détection d'autant plus efficaces qu'ils seront originaux, confidentiels et adaptés aux circonstances rencontrées.*

Ces extraits ont été publiés par la revue Partis Pris et le syndicat parisien CFDT de la Sécurité sociale... sans aucune réaction !