Recommandation 1210 (1993)[1]

Systèmes informatisés à risque

Assemblée parlementaire

1. L'Assemblée a conscience que l'utilisation des ordinateurs pour des applications liées à la sûreté se développe, notamment dans des domaines comme les systèmes de contrôle des avions, des trains à grande vitesse et des centrales nucléaires, les équipements et les registres médicaux, les systèmes de freins antiblocage des véhicules et d'autres applications de génie mécanique en général, et enfin et surtout les armes modernes et leurs systèmes de guidage.

2. De nombreux accidents récents (par exemple accident d'avion dû à une panne informatique, robot déréglé tuant un opérateur, décès de malade à la suite du dysfonctionnement d'un goutte-à-goutte commandé par ordinateur, échec du lancement d'une fusée en raison d'une erreur de programme, piraterie de logiciel, etc.) inquiètent le public et remettent en question la fiabilité de ces systèmes.

3. Nul doute qu'il existe aux niveaux professionnel et scientifique un profond souci de garantir la sûreté de ces systèmes automatiques sophistiqués. Il n'en demeure pas moins que les priorités économiques et budgétaires peuvent parfois avoir le dessus dans l'industrie, aux dépens des autres facteurs. Par conséquent, la question de la sûreté doit être considérée comme un domaine d'intérêt public.

4. La sûreté est une notion difficile à saisir. Elle est étroitement liée à celles de danger et de risque. La sûreté absolue n'existe pas. Toute activité humaine comporte un certain degré de risque et les créations technologiques n'échappent pas à cette règle. L'important c'est de réduire ces risques dans la mesure du possible et d'éclairer le public.

5. Le plus souvent, les systèmes de contrôle de sûreté ne sont couverts par aucun règlement spécifique, et le contrôle de la qualité n'est effectué que par des procédures internes propres aux secteurs d'industries concernés. En outre, les codes mathématiques qui étayent les logiciels de ces systèmes relèvent souvent du secret commercial, rendant ainsi toute enquête difficile.

6. Il serait effectivement beaucoup plus rentable que l'industrie consacre davantage d'efforts et de fonds à la phase de conception, phase cruciale pour la mise au point de systèmes complexes. A défaut, la fixation de normes, de règles et de sanctions peut néanmoins avoir un effet dissuasif contre les «raccourcis» technologiques.

7. Les «Lignes directrices régissant la sécurité des systèmes d'information», récemment élaborées par l'OCDE, témoignent d'une sensibilité accrue vis-à-vis des problèmes posés par l'utilisation diverse des ordinateurs. Elles sont néanmoins axées sur les aspects de la protection des données afin qu'il ne soit pas porté atteinte au niveau de confidentialité, de disponibilité et d'intégrité des systèmes en question. Elles doivent être complétées par une étude du problème en amont, c'est-à-dire par une étude de la fiabilité technologique.

1. Texte adopté par la Commission Permanente, agissant au nom de l'Assemblée, le 26 mars 1993. Voir Doc. 6792, rapport de la commission de la science et de la technologie, rapporteur: M. Fulvio Caccia.

8. Pour les raisons qui précèdent, l'Assemblée recommande au Comité des Ministres d'inviter les gouvernements des Etats membres à entreprendre une activité de caractère interdisciplinaire au sein de l'OCDE, et en particulier au sein de sa direction de la science, de la technologie et de l'industrie, dont le but serait:

8.1. de déterminer les domaines qui présentent un intérêt public, en y incluant les technologies de l'avenir actuellement en cours d'élaboration, telles que les communications informatiques entre la route et les véhicules, le système ferroviaire paneuropéen, etc.;

8.2. d'établir un inventaire européen et une analyse de certains accidents majeurs dus aux systèmes informatisés;

8.3. de dresser une liste des normes nationales et internationales existantes, et des législations spécifiques là où elles existent;

8.4. de préparer un lexique des notions techniques et juridiques afin que les législations futures soient compatibles avec la réalité extrêmement complexe des systèmes technologiques en question;

8.5. d'élaborer des principes généraux concernant les méthodes d'évaluation de la sûreté dans les premiers stades de la conception des produits et des systèmes complexes;

8.6. de mettre au point les grandes lignes d'une formation adaptée pour ceux qui ont la responsabilité sur les plans national et européen d'évaluer et de juger les effets sur la sûreté des technologies nouvelles, formation qui doit avoir un caractère multidisciplinaire et inclure une connaissance approfondie des paramètres économiques;

8.7. de mener à bien une étude sur la comparaison et l'amélioration des législations relatives à la détermination des responsables en cas d'accident;

8.8. de prévoir des mesures spéciales pour les enquêtes scientifiques et judiciaires dans le cadre des règles de protection de la propriété intellectuelle;

8.9. de mettre en place, le cas échéant et une fois les connaissances nécessaires acquises grâce aux recherches initiales, un contrôle de la qualité et des systèmes de certification, tant au niveau national qu'au niveau européen, cela en s'inspirant de l'expérience déjà acquise dans le domaine de normalisation électrotechnique grâce aux travaux de la Commission électrotechnique internationale (CEI) et du Comité européen de normalisation électrotechnique (CENELEC).