

Système d'interception Echelon

2001/2098(INI) - 03/07/2001

La commission temporaire sur le système d'interception Echelon a adopté le rapport d'initiative de M. Gerhard SCHMID (PSE, D) clôturant un an de travaux. La première tâche du mandat confiée à la commission temporaire était de vérifier l'existence de ce système d'interception. Si aucune preuve formelle n'existe, au vu des indices et des déclarations concordantes provenant notamment de sources américaines, l'existence d'un tel système mondial "avec la participation des Etats-Unis, du Royaume-Uni, du Canada, de l'Australie et de la Nouvelle-Zélande, dans le cadre de l'accord UKUSA, ne fait plus de doute". Il en va de même pour l'utilisation Echelon, à savoir que ce système est bien employé "pour intercepter des communication privées et économiques mais non militaires". Si les capacités de ce système ne sont pas aussi vastes que ce que les médias ont parfois avancé, les parlementaires s'inquiètent toutefois que de nombreux responsables communautaires auditionnés aient déclaré ne pas connaître ce système. La deuxième tâche était de vérifier la compatibilité avec le droit communautaire. Le rapport fait une distinction entre les activités de renseignements qui sont licites et l'emploi d'un tel système pour espionner les communications des entreprises. Dans un tel cas, l'état membre qui participerait à une telle démarche violerait le droit de l'UE. Si les travaux de la commission n'ont pas permis de mettre en lumière des preuves démontrant que le système d'interception mondial était utilisé afin de fausser les conditions de concurrence, le rapport indique cependant que, selon les informations recueillies aux USA : "5% des informations collectées grâce à des sources non publiques sont utilisées à des fins économiques (...) cette surveillance pourrait permettre aux entreprises des Etats-Unis d'emporter jusqu'à 7 milliards de dollars de marchés". Le rapport précise que les données sensibles étant essentiellement à l'intérieur des entreprises, on utilise d'autres méthodes d'espionnage. Ce n'est en fait que lorsque les informations sont acheminées vers l'extérieur qu'une surveillance des communications peut se révéler efficace. A ce propos, le rapport invite les Etats membres et le gouvernement des Etats-Unis à nouer un dialogue franc sur la collecte de renseignements économiques. Un autre volet du mandat concernait la protection de la vie privée et les éventuelles initiatives politiques ou législatives que la commission pourraient dégager de ses travaux. A cet égard, la commission demande aux Etats membres de garantir à tous les citoyens les mêmes garanties légales face aux écoutes. Il s'agit également de vérifier la conformité de leur législation sur les services de renseignements avec la Convention européenne relative aux droits de l'homme et avec la jurisprudence de la Cour des droits de l'homme. Enfin, de se doter d'instruments contraignants garantissant une protection effective contre toute forme d'interception extralégale de leurs communications. A propos des services de renseignements, le rapport souligne la nécessité de voir tous les parlements nationaux disposer d'organes de contrôle de ces services. Par ailleurs, les Etats membres devraient mettre en commun leurs moyens d'interceptions des communications afin de renforcer l'efficacité de la PESD dans les domaines du renseignement et dans la lutte contre le terrorisme et la criminalité, "sous le contrôle du Parlement européen, du Conseil et de la Commission". Par ailleurs, l'Allemagne et le Royaume-Uni sont invités à subordonner l'autorisation d'interception sur leur territoire par les services de renseignement américains à certaines conditions. La commission souligne l'importance de sensibiliser les particuliers et les entreprises afin de leur faire prendre conscience des risques potentiels et de la nécessité de se protéger contre le danger de voir leurs communications interceptées. Une série de propositions pratiques sont faites à cet égard, notamment la nécessité de soutenir le développement de logiciels de cryptage européens. La Commission est invitée à prendre une série de mesures : procéder à une analyse de sécurité, actualiser son système de cryptage, assurer la protection des données dans leur traitement interne, renforcer la protection des documents non publics. Enfin, la Commission devrait proposer la création, en collaboration avec les entreprises et les Etats membres, d'un réseau européen et coordonné de centres de conseil en matière de sécurité de l'information dans les entreprises qui, au-delà de la sensibilisation, pourrait leurs apporter une aide pratique. Les entreprises sont d'ailleurs invitées à coopérer d'avantage avec les services de contre-espionnage en leur signalant les éventuelles attaques extérieures dont elles estiment avoir été victime.