ASSEMBLÉE NATIONALE

11ème législature

réseaux de données

Question écrite n° 7158

Texte de la question

Le 25 août 1997, le Premier ministre a exprimé son intention de libéraliser le régime de la cryptologie. Cette décision était attendue depuis longtemps et elle apparaît comme judicieuse dans la mesure où la réglementation française de la cryptologie, telle qu'elle résulte de la loi n° 96-659 du 26 juillet 1996, est l'une des plus restrictives au monde ; ni l'Allemagne, ni le Royaume-Uni, ni les Etats-Unis n'imposent quelque restriction que ce soit à l'utilisation de moyens ou de services de cryptologie. Il est ainsi surprenant que le cryptage à 40 bits soit toujours soumis à autorisation alors qu'il constitue désormais un standard commercial international et qu'il ne représente aucune menace pour la sécurité de notre pays. Il est tout aussi surprenant que, d'après certaines informations disponibles sur les projets de décrets d'application de la loi du 26 juillet 1996, les moyens de cryptage à 40 bits soient dans le futur toujours soumis à la procédure de déclaration préalable. Les restrictions qui frappent la commercialisation des moyens et des services cryptologiques à 40 bits engendrent surcoûts et délais supplémentaires pour les éditeurs et vendeurs de logiciels informatiques. Elles aboutissent à priver les sociétés françaises de moyens de communication offrant un niveau minimum de sécurité, ce qui les rend vulnérables à l'espionnage industriel ainsi qu'au piratage informatique. En ce qui concerne l'obligation imposée aux utilisateurs de moyens et de services de cryptologie de faire séquestrer leurs clefs de chiffrement auprès de « tiers de confiance », celle-ci semble totalement injustifiée dans le cas du cryptage à 40 bits. En effet, les services spécialisés français disposent déjà d'un large accès à une importante documentation technique qui leur permet, si besoin est, de décrypter facilement en temps réel toute communication cryptée à 40 bits. Par ailleurs, il apparaît que le développement du commerce électronique repose essentiellement sur la diffusion de moyens de cryptologie répondant à des standards internationaux qui permettent d'assurer non seulement l'authentification et l'intégrité des transactions et des paiements mais aussi la confidentialité des échanges commerciaux. Les systèmes réglementaires complexes visant à limiter les moyens de cryptologie, soit en restreignant leur diffusion, soit en limitant leurs capacités, devraient être cantonnés aux messages cryptés ne transitant pas par des entités responsables (telles les banques, les organismes émetteurs de cartes de crédit ou les commerçants) puisque ces entités font déjà l'objet de réglementations particulières qui permettent de les contrôler. M. Yann Galut demande si M. le secrétaire d'Etat à l'industrie pourrait ainsi lui confirmer que : a) Les décrets devant être promulgués avant la fin de l'année en vue de l'application de l'article 17 de la loi n° 96-659 du 26 juillet 1996 permettront une rapide diffusion de moyens de cryptologie afin de développer de façon significative le commerce électronique en France ? b) Les préoccupations techniques et commerciales émanant tant des professionnels de l'édition de logiciels informatiques que des professionnels du commerce électronique ont bien été prises en compte dans la rédaction des décrets ? En outre, pourrait-il rassurer l'Assemblée en confirmant que : c) Les moyens de cryptage à 40 bits qui constituent d'ores et déjà un standard commercial et qui ne représentent aucune menace pour la sécurité de notre pays ne seront pas soumis à un contrôle préalable, que ce soit sous forme d'autorisation ou de déclaration, qui aurait pour effet d'empêcher ou de retarder l'introduction en France de technologies cruciales pour le développement du commerce électronique, des entreprises et de l'emploi ? d) Les exigences relatives à la mise sous séquestre de clefs de cryptage seront limitées aux personnes ayant recours à des moyens ou services de cryptologie dans un cadre autre que commercial ?

Texte de la réponse

S'il est vrai que des pays comme l'Allemagne, le Royaume-Uni ou les Etats-Unis ne disposent pas pour l'instant d'outils législatifs leur permettant de contrôler l'usage de la cryptologie, il est cependant utile de noter que ces pays, comme beaucoup d'autres, sont soumis actuellement à des débats internes, parfois vigoureux, sur la mise en place d'un contrôle minimum. Cette approche est inéluctable si l'on ne veut pas que les autoroutes de l'information deviennent des zones de non-droit sur lesquelles des informations de toutes natures (terrorisme, blanchiment d'argent, pédophilie, etc.) pourront circuler en toute impunité. Ainsi, si les pays partent de niveaux différents (absence de réglementation pour l'Allemagne ou réglementation très restrictive pour la France), il y a un consensus au niveau international sur la nécessité de trouver un juste milieu entre les contraintes industrielles, commerciales et de vie privée, et celles liées à l'ordre public et à la sécurité des Etats. Dans sa recommandation R. 95-13 (Problèmes des procédures légales anticriminalité liés aux technologies de l'information) du 11 septembre 1995, le Conseil de l'Europe a bien mis en évidence cette nécessité de trouver des mesures minimisant les effets de l'usage de la cryptographie sur les enquêtes criminelles, sans que ces mesures aillent au-delà de ce qui est strictement nécessaire. Le secrétaire d'Etat à l'industrie peut confirmer à l'honorable parlementaire que c'est bien dans ce sens d'un assouplissement que va la nouvelle législation nationale, en cours de mise en place, en matière de moyens et de prestations de cryptologie (art. 17 de la loi de réglementation des télécommunications du 26 juillet 1996 ainsi que les décrets et arrêtés correspondants, en cours de promulgation). Par rapport à la loi de décembre 1990 et aux décrets de 1992, en plus du régime de demande d'autorisation sont créés deux régimes plus souples au titre desquels certains moyens ou prestations de cryptologie peuvent être soumis uniquement à déclaration, soit dispensés purement et simplement de toute formalité. Les produits « 40 bits » notamment seront libres d'utilisation et leur fourniture sera soumise à un simple régime déclaratif qui, tout en étant plus souple que le régime de demande d'autorisation est nécessaire pour pouvoir vérifier que ces produits n'ont pas d'autres finalités que celles affichées officiellement par leurs concepteurs. Le secrétaire d'Etat à l'industrie reste persuadé que ce système législatif dans son ensemble constitue un progrès important dans la recherche de l'équilibre ci-dessus entre, d'une part, besoins commerciaux et privés, et, d'autre part, nécessités d'ordre public et de sécurité nationale.

Données clés

Auteur : M. Yann Galut
Circonscription : Cher (3e circonscription) - Socialiste
Type de question : Question écrite
Numéro de la question : 7158
Rubrique : Télécommunications
Ministère interrogé : industrie
Ministère attributaire : industrie

Date(s) clée(s)

Question publiée le : 1er décembre 1997, page 4320
Réponse publiée le : 9 février 1998, page 726