

ORGANISATION MONDIALE DU COMMERCE

G/TBT/Notif.97.584

30 septembre 1997

(97-4099)

Comité des obstacles techniques au commerce

NOTIFICATION

La notification suivante est communiquée conformément à l'article 10.6.

1.	Membre de l'Accord adressant la notification: <u>FRANCE</u> Le cas échéant, pouvoirs publics locaux concernés (articles 3.2 et 7.2):
2.	Organisme responsable: Service des industries de communication et de service 3/5, rue Barbet de Jouy 75353 Paris 07 SP L'organisme ou l'autorité désigné pour s'occuper des observations concernant la notification peut être indiqué s'il est différent de l'organisme susmentionné:
3.	Notification au titre de l'article 2.9.2 [X], 2.10.1 [], 5.6.2 [], 5.7.1 [], autres:
4.	Produits visés (le cas échéant, position du SH ou de la NCCD, sinon position du tarif douanier national. Les numéros de l'ICS peuvent aussi être indiqués, le cas échéant): Services et matériels associés aux clés de chiffrement
5.	Intitulé, nombre de pages et langue(s) du texte notifié: Projet de décret définissant les conditions dans lesquelles sont agréés les organismes gérant, pour le compte d'autrui, des conventions secrètes de moyens ou de prestations de cryptologie permettant d'assurer des fonctions de confidentialité.
6.	Teneur: Les dispositions du texte ont pour but d'instaurer, en sus des autres modes de chiffrement, la fonction d'organisme agréé en tant que tierce partie de confiance (TPC) en cryptologie, dont le rôle est de mettre à disposition des utilisateurs les clés de chiffrement nécessaires au fonctionnement de leurs moyens de chiffrement, de définir les fonctionnalités des TPC et de préciser la procédure administrative d'agrément de cet organisme.

7. Objectif et justification: Le texte est pris en application de l'article 28 de la Loi de réglementation des télécommunications du 29 décembre 1990, modifié par l'article 17 de la Loi de réglementation des télécommunications du 26 juillet 1996. Ses dispositions sont indispensables pour la mise en oeuvre des obligations et procédures prévues par la loi, au sujet des TPC.

Les dispositions de la réglementation touchant à l'usage de la cryptologie doivent être aujourd'hui assouplies. En effet le développement des autoroutes de l'information va entraîner une augmentation considérable des transactions électroniques qui ont besoin d'être sécurisées afin de garantir leur fiabilité et leur confidentialité.

L'Etat doit par ailleurs se préoccuper de conserver les instruments qui contribuent à la sécurité publique, tels que les interceptions.

Aussi la nouvelle législation se propose de simplifier considérablement la possibilité, pour l'utilisateur final, de recourir à des moyens de cryptologie, alors que jusqu'à présent une autorisation explicite est le plus souvent nécessaire.

La liberté sera totale d'utiliser les moyens de cryptologie pour rendre confidentiel un message à condition que les prestations de confidentialité employées soient gérées par un TPC.

Le TPC est un organisme habilité qui gère des clés de chiffrement pour le compte de l'utilisateur. Ce dernier passe un contrat avec le tiers de confiance qui lui transmet régulièrement les clés à utiliser pour chiffrer son information. Dans la licence du tiers de confiance figure une clause par laquelle celui-ci doit remettre les clés de chiffrement aux autorités habilitées en vertu de la loi. Ainsi l'utilisateur peut-il s'appuyer sur un professionnel de la cryptologie qui lui garantit un service de haute qualité, tandis que l'Etat peut, en cas de besoin, accéder au contenu de l'information.

Ces dispositions libérales qui intéressent l'utilisateur font porter le poids de la réglementation sur les professionnels de la cryptologie. Ceux-ci doivent informer les pouvoirs publics des instruments qu'ils mettent sur le marché. Ils doivent aussi demander une autorisation s'ils veulent devenir tiers de confiance. Ils sont tenus à un strict respect des règles auxquelles ils ont souscrit et des dispositions pénales particulières sont prévues s'ils ne s'y conformaient pas.

8. Documents pertinents:

- article 28 de la Loi de réglementation des télécommunications du 29 décembre 1990
- article 17 de la Loi de réglementation des télécommunications du 26 juillet 1996

9. Date projetée pour l'adoption: } décembre 1997
Date projetée pour l'entrée en vigueur: }

10. Date limite pour la présentation des observations: 24 novembre 1997

11. Entité auprès de laquelle le texte peut être obtenu: point national d'information [X] ou adresse et numéro de télégramme d'un autre organisme: (CINORTECH)

Mme Vacher (AFNOR)
Tour Europe
92049 Paris La Défense