RECOMMANDATION DU CONSEIL RELATIVE AUX LIGNES DIRECTRICES RÉGISSANT LA POLITIQUE DE CRYPTOGRAPHIE

le 27 Mars 1997

LE CONSEIL

VU :

– la Convention relative à l'Organisation de Coopération et de Développement Economiques, en date du 14 décembre 1960, et notamment ses articles 1 b), 1 c), 3 a) et 5 b) ;

– la Recommandation du Conseil concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, en date du 23 septembre 1980 [C(80)58(Final)] ;

– la Déclaration sur les flux transfrontières de données adoptée par les gouvernements des pays Membres de l'OCDE le 11 avril 1985 [C(85)139, Annexe] ;

– la Recommandation du Conseil concernant les Lignes directrices régissant la sécurité des systèmes d'information des 26 et 27 novembre 1992 [C(92)188/FINAL] ;

– la Directive [95/46/CE] du Parlement Européen et du Conseil de l'Union Européenne du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

– l'Arrangement de Wassenaar sur le contrôle des exportations des armes conventionnelles et des biens et technologies à double usage convenu le 13 juillet 1996 ;

– le Règlement [(CE) 3381/94] et la Décision [94/942/PESC] du Conseil de l'Union européenne du 19 décembre 1994 concernant le contrôle des exportations de biens à double usage ;

– et la Recommandation [R(95)13] du Conseil de l'Europe du 11 septembre 1995 relative aux problèmes de procédure pénale liés à la technologie de l'information ;

CONSIDÉRANT **:**

– que les infrastructures nationales et mondiales de l'information se développent rapidement de manière à offrir un réseau continu pour les communications et l'accès aux données, à l'échelle mondiale ;

– que l'émergence de ce réseau d'information et de communication est susceptible d'avoir un impact important sur le développement économique et le commerce mondial ;

– que les utilisateurs des technologies de l'information doivent avoir confiance dans la sécurité des infrastructures, des réseaux et des systèmes d'information et de communication ; dans la confidentialité, l'intégrité et la disponibilité des données sur ces systèmes, ainsi que dans la possibilité de prouver l'origine et la réception des données ;

– que les données sont de plus en plus vulnérables à des menaces sur leur sécurité mettant en jeu des moyens perfectionnés, et que le fait d'assurer la sécurité des données par le biais de la législation, de la procédure ou de la technique revêt une importance fondamentale pour que les infrastructures nationales et internationales de l'information concrétisent toutes leurs promesses ;

RECONNAISSANT **:**

– que la cryptographie, du fait qu'elle peut être un outil efficace pour un usage sûr des technologies de l'information en garantissant la confidentialité, l'intégrité et la disponibilité des données et en fournissant des mécanismes pour l'authentification et la non-répudiation de ces données, constitue un élément important pour rendre sûrs les réseaux et systèmes d'information et de communication ;

– que la cryptographie a diverses applications liées à la protection de la vie privée, de la propriété intellectuelle, des informations commerciales et financières, de la sécurité publique et de la sécurité nationale ainsi qu'à la pratique du commerce électronique, notamment les transactions et paiements anonymes sûrs ;

– que le fait de ne pas utiliser des méthodes cryptographiques peut nuire à la protection de la vie privée, de la propriété intellectuelle, des informations commerciales et financières, de la sécurité publique et de la sécurité nationale ainsi qu'à la pratique du commerce électronique, car les données et les communications peuvent être insuffisamment protégées contre les accès non autorisés, les modifications et les utilisations abusives, et les utilisateurs peuvent donc de ne pas avoir confiance dans les infrastructures, réseaux et systèmes d'information et de communication ;

– que l'utilisation de la cryptographie pour garantir l'intégrité des données, y compris les mécanismes d'authentification et de non-répudiation, peut être distinguée de son utilisation pour garantir la confidentialité des données, et que chacune de ces utilisations pose des problèmes différents ;

– que la qualité de la protection de l'information assurée par la cryptographie dépend non seulement des moyens techniques retenus, mais aussi du respect de bonnes procédures en matière de gestion, d'organisation et d'exploitation ;

RECONNAISSANT EN OUTRE :

– que les gouvernements ont de vastes responsabilités et que l'utilisation de la cryptographie a des implications évidentes pour plusieurs d'entre elles, s'agissant notamment de protéger la vie privée et de faciliter la sécurité des systèmes d'information et de communication ; de promouvoir le bien-être économique, en encourageant notamment le commerce ; d'assurer la sécurité publique ; et de veiller au respect des lois et d'assurer la sécurité nationale ;

– qu'il existe, pour les gouvernements, les entreprises et les particuliers, des besoins et des usages légitimes de la cryptographie, mais que la cryptographie peut aussi être utilisée par des personnes physiques ou morales pour des activités illégales, ce qui peut affecter la sécurité publique, la sécurité nationale, le respect des lois, l'activité commerciale, la vie privée ou la protection du consommateur, et

que les gouvernements, en liaison avec l'industrie et le grand public, se doivent donc de dégager une politique qui concilie ces intérêts ;

– qu'en raison du caractère intrinsèquement mondial des réseaux d'information et de communication, l'introduction de politiques nationales incompatibles ne répondra pas aux attentes des particuliers, des entreprises et des gouvernements et peut créer des obstacles à la coopération et au développement économiques ; et il se peut donc que les politiques nationales doivent être coordonnées au plan international ;

– que la présente Recommandation du Conseil ne saurait affecter les droits souverains des gouvernements nationaux, et que les Lignes directrices jointes en annexe à ladite Recommandation demeurent régies par la législation nationale ;

Sur la proposition du Comité de la politique de l'information, de l'informatique et des communications ;

RECOMMANDE AUX PAYS MEMBRES :

1. d'établir des politiques, méthodes, mesures, pratiques et procédures nouvelles ou de modifier celles qui existent de manière à refléter et prendre en compte les principes relatifs à la politique de cryptographie énoncés dans les Lignes directrices figurant dans l'annexe à la présente Recommandation (ci-après appelées "les Lignes directrices"), dont elle fait partie intégrante ; et ce faisant, de prendre également en compte la Recommandation du Conseil concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, en date du 23 septembre 1980 [C(80)58(Final)] et la Recommandation du Conseil concernant les Lignes directrices régissant la sécurité des systèmes d'information, en date des 26 et 27 novembre 1992 [C(92)188/FINAL] ;

2. de se consulter, de coordonner leur action et de coopérer aux échelons national et international dans la mise en oeuvre des Lignes directrices ;

3. de répondre au besoin de solutions pratiques et opérationnelles dans le domaine de la politique internationale de cryptographie en utilisant les Lignes directrices comme base pour des accords sur des questions spécifiques liées à la politique internationale de cryptographie ;

4. de diffuser les Lignes directrices dans l'ensemble des secteurs public et privé afin de contribuer à la sensibilisation aux questions et politiques liées à la cryptographie ;

5. de veiller à la levée, ou d'éviter de créer au nom de la politique de cryptographie, des obstacles injustifiés au commerce international et au développement des réseaux d'information et de communication ;

6. d'énoncer clairement et de rendre publique toute mesure nationale de contrôle affectant l'utilisation de la cryptographie ;

7. de réexaminer les Lignes directrices au moins tous les cinq ans en vue d'améliorer la coopération internationale sur les questions concernant la politique de cryptographie.