Recommandation du Conseil relative aux Lignes directrices régissant la politique de cryptographie

Instruments juridiques de l'OCDE

DES POLITIQUES MEILLEURES
POUR UNE VIE MEILLEURE

Ce document est publié sous la responsabilité du Secrétaire général de l’OCDE. Il reproduit un instrument juridique de l'OCDE et peut contenir des informations complémentaires. Les opinions ou arguments exprimés dans ces informations complémentaires ne reflètent pas nécessairement les vues officielles des pays Membres de l’OCDE.

Ce document, ainsi que les données et cartes qu'il peut comprendre, sont sans préjudice du statut de tout territoire, de la souveraineté s'exerçant sur ce dernier, du tracé des frontières et limites internationales, et du nom de tout territoire, ville ou région.

Pour accéder aux textes officiels à jour des instruments juridiques de l’OCDE, ainsi qu’aux informations s’y rapportant, veuillez consulter le Recueil des instruments juridiques de l’OCDE http://legalinstruments.oecd.org.

Merci de citer cet ouvrage comme suit :
OCDE, *Recommandation du Conseil relative aux Lignes directrices régissant la politique de cryptographie*, OECD/LEGAL/0289

Collection : Instruments juridiques de l’OCDE

Crédits photo : © Adobe Stock/Cousin_Avi

© OECD 2025

Ce document est mis à disposition à titre gratuit. Il peut être reproduit et distribué gratuitement sans autorisation préalable à condition qu'il ne soit modifié d'aucune façon. Il ne peut être vendu.

Ce document est disponible dans les deux langues officielles de l'OCDE (anglais et français). Il peut être traduit dans d’autres langues à condition que la traduction comporte la mention "traduction non officielle" et qu’elle inclut l'avertissement suivant : *"Cette traduction a été préparée par [NOM DE L'AUTEUR DE LA TRADUCTION] à des fins d'information seulement et son exactitude ne peut être garantie par l'OCDE. Les seules versions officielles sont les textes anglais et français disponibles sur le site Internet de l'OCDE http://legalinstruments.oecd.org"*

Informations Générales

La Recommandation relative aux Lignes directrices régissant la politique de cryptographie (ci-après « la Recommandation ») a été adoptée par le Conseil de l'OCDE le 27 mars 1997 sur proposition du Comité de l'information, de l'informatique et des communications (désormais appelé Comité de la politique du numérique).

La nécessité d'une norme sur la politique de cryptographie

La cryptographie désigne l'ensemble des principes, moyens et méthodes de transformation des données destinés à dissimuler leur contenu, établir leur authenticité, empêcher que leur modification passe inaperçue, prévenir leur répudiation et empêcher et/ou prévenir leur utilisation non autorisée. C'est l'un des moyens technologiques d'assurer la sécurité des données dans les systèmes d'information et de communication ainsi que la confiance dans les activités économiques et sociales qui reposent sur de telles données.

La cryptographie peut être utilisée pour protéger la confidentialité de données, telles que données de caractère financier ou personnel, qu'il s'agisse de données mémorisées ou de données en transit. La cryptographie peut aussi servir à vérifier l'intégrité des données en révélant les cas d'altération et en identifiant la personne ou le dispositif qui est l'auteur de l'envoi. Ces techniques sont au centre du développement et de l'utilisation des technologies et des réseaux et des technologies d'information et de communication nationaux et mondiaux.

Dans les années 1990, les pays Membres de l'OCDE entreprirent d'élaborer et de mettre en œuvre des politiques et des législations à l'égard de la cryptographie ; dans de nombreux pays, ce processus était toujours en cours en 1997. Étant donné que les disparités entre les politiques peuvent créer des obstacles à l'évolution des réseaux numériques et freiner le développement du commerce international, les pays Membres de l'OCDE prirent conscience de la nécessité d'une approche coordonnée au niveau international pour faciliter le bon développement d'une infrastructure de l'information sûre et efficace.

L'OCDE joue un rôle important à cet égard en édifiant un consensus sur certains problèmes spécifiques de politique générale et de réglementation à l'égard des technologies et réseaux d'information et de communication, notamment sur les questions de cryptographie.

En 1997, l'OCDE œuvrait depuis un certain temps dans les domaines relatifs à la confiance dans l'environnement numérique, y compris avec l'adoption de la Recommandation concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel en 1980 [OECD/LEGAL/0188] et avec la Recommandation concernant les Lignes directrices régissant la sécurité des systèmes d'information en 1992 [OECD/LEGAL/0271].

Processus pour le dévelopment de la Recommandation

Au début de 1996, l'OCDE a lancé un projet sur la politique de cryptographie en constituant un Groupe ad hoc d'experts sur les Lignes directrices régissant la politique de cryptographie (ci-après appelé le "Groupe ad hoc") sous les auspices du Comité de la politique de l'information, de l'informatique et des communications, désormais appelé Comité de la politique du numérique (CPN).

Le Groupe ad hoc, présidé par Mr. Norman Reaburn du department du procureur général de l'Australie, a été chargé de la rédaction d'un projet de lignes directrices régissant la politique de cryptographie pour mettre en lumière les questions dont il devrait être tenu compte dans la formulation des politiques sur la cryptographie aux échelons national et international. Le Groupe ad hoc a reçu un mandat d'un an pour accomplir cette tâche et il a achevé ses travaux en décembre 1996. Par la suite, les Lignes directrices régissant la politique de cryptographie ("les Lignes directrices") ont été adoptées en tant que Recommandations du Conseil et sont devenues effectives le 27 mars 1997.

Portée de la Recommandation

Les Lignes Directrices figurant à l'annexe à la Recommandation, dont elles font partie intégrante, couvrent un large domaine et témoignent de la diversité des opinions parmi les Adhérents.

Elles visent à promouvoir l'utilisation de la cryptographie de manière à favoriser la confiance dans les technologies numériques ainsi que dans la manière dont ils sont utilisés, sans mettre indûment en péril la sécurité publique, le respect des lois et la sécurité nationale.

Elles visent également à mieux faire prendre conscience du besoin de politiques et législations compatibles en matière de cryptographie ; à promouvoir la coopération entre les secteurs public et privé dans la mise au point et l'application de politiques, méthodes, mesures, pratiques et procédures nationales et internationales relatives à la cryptographie ; à faciliter les échanges internationaux en soutenant des systèmes cryptographiques qui assurent l'interopérabilité, la portabilité et la mobilité, et sont d'un bon rapport coût-efficacité ; et à promouvoir la coopération internationale entre les pouvoirs publics, les milieux d'affaires, la communauté de la recherche et les organisations de normalisation pour parvenir à une utilisation concertée des méthodes cryptographiques.

Pour plus d'informations, merci de consulter : https://www.oecd.org/fr/sti/ieconomie/security.htm

Contact : digitalsecurity@oecd.org.

Mise en œuvre

Lors de l'adoption de la Recommandation, le Conseil de l'OCDE a chargé le Comité de la politique du numérique (CPN) d'examiner les Lignes directrices au moins tous les cinq ans en vue d'améliorer la coopération internationale sur les questions relatives à la politique de cryptographie. Par conséquent, pour le premier examen en 2002, un questionnaire fut diffusé aux Adhérents pour s'enquérir quant au besoin de modifications, additions ou suppressions de certaines parties des Lignes directrices. Un questionnaire similaire fut réutilisé pour les examens de 2007, 2012 et 2017. Tous ces examens ont conclu que les Lignes directrices étaient adéquates pour traiter les questions et les finalités pour lequelles elles furent formulées et qu'il n'était pas nécessaire de les réviser.

LE CONSEIL,

VU :

la Convention relative à l'Organisation de coopération et de développement économiques, 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 œuvre 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.

ANNEXE

LIGNES DIRECTRICES REGISSANT LA POLITIQUE DE CRYPTOGRAPHIE

I. Finalités

Les Lignes directrices visent à :

- promouvoir l'utilisation de la cryptographie, de manière à :
    - favoriser la confiance dans les infrastructures, réseaux et systèmes d'information et de communication, ainsi que dans la manière dont ils sont utilisés ;
    - contribuer à assurer la sécurité des données, et à protéger la vie privée, dans les infrastructures, réseaux et systèmes d'information et de communication nationaux et mondiaux ;
- promouvoir cette utilisation de la cryptographie sans mettre indûment en péril la sécurité publique, le respect des lois et la sécurité nationale ;
- mieux faire prendre conscience du besoin de politiques et législations compatibles en matière de cryptographie, ainsi que de méthodes cryptographiques assurant l'interopérabilité, la portabilité et la mobilité dans les réseaux d'information et de communication nationaux et mondiaux ;
- aider les décideurs des secteurs public et privé dans l'élaboration et la mise en œuvre de politiques, méthodes, mesures, pratiques et procédures nationales et internationales cohérentes pour une utilisation efficace de la cryptographie ;
- promouvoir la coopération entre les secteurs public et privé dans la mise au point et l'application de politiques, méthodes, mesures, pratiques et procédures nationales et internationales relatives à la cryptographie ;
- faciliter les échanges internationaux en soutenant des systèmes cryptographiques qui assurent l'interopérabilité, la portabilité et la mobilité, et sont d'un bon rapport coût-efficacité ;
- promouvoir la coopération internationale entre les pouvoirs publics, les milieux d'affaires, la communauté de la recherche et les organisations de normalisation pour parvenir à une utilisation concertée des méthodes cryptographiques.

II. Champ d'application

Les Lignes directrices s'adressent principalement aux gouvernements, du fait des recommandations d'action qu'elles contiennent, étant entendu toutefois qu'elles seront largement consultées et suivies tant par le secteur public que par le secteur privé.

Il est admis que les gouvernements ont des responsabilités dissociables et distinctes s'agissant de protéger l'information dont la sécurité doit être assurée dans l'intérêt national; les Lignes directrices n'ont pas vocation à s'appliquer dans ces domaines.

III. Définitions

Aux fins des Lignes directrices, l'expression :

« Authentification » signifie une fonction pour l'établissement de la validité de l'identité déclarée d'un utilisateur, d'un dispositif ou d'une autre entité dans un système d'information ou de communication.

« Disponibilité » signifie la propriété que les données, l'information et les systèmes d'information et de communication sont accessibles et utilisables en temps voulu et de la manière requise.

« Confidentialité » signifie la propriété que des données ou une information ne sont ni rendues disponibles, ni divulguées aux personnes, entités ou processus non autorisés.

« Cryptographie » signifie la discipline incluant les principes, moyens et méthodes de transformation des données dans le but de cacher leur contenu sémantique, d'établir leur authenticité, d'empêcher que leur modification passe inaperçue, de prévenir leur répudiation et d'empêcher leur utilisation non autorisée.

« Clé cryptographique » signifie un paramètre utilisé avec un algorithme cryptographique pour transformer, valider, authentifier, chiffrer ou déchiffrer des données.

« Méthodes cryptographiques » désigne les techniques, services, systèmes, et produits cryptographiques et les systèmes de gestion de clés.

« Données » signifie la représentation d'informations d'une manière adaptée à la communication, à l'interprétation, au stockage ou au traitement.

« Déchiffrement » signifie la fonction inverse du chiffrement.

« Chiffrement » signifie la transformation de données au moyen de la cryptographie pour rendre celles-ci inintelligibles (données chiffrées) afin d'en assurer la confidentialité.

« Intégrité » signifie la propriété que les données ou l'information n'ont pas été modifiées ou altérées de manière non autorisée.

« Interopérabilité » des méthodes cryptographiques signifie la capacité pour de multiples méthodes cryptographiques de techniquement fonctionner ensemble.

« Système de gestion de clés » signifie un système de production, de stockage, de distribution, de reprise, de suppression, d'archivage, de certification ou d'application des clés cryptographiques.

« Détenteur de clés » signifie une personne ou entité qui possède ou contrôle des clés cryptographiques. Un détenteur de clé n'est pas nécessairement utilisateur de la clé.

Le « respect des lois » fait référence à toutes les lois, quel qu'en soit l'objet.

« Accès légal » signifie l'accès au texte en clair, ou aux clés cryptographiques, de données chiffrées, dont bénéficie des tierces personnes, physiques ou morales, notamment des entités gouvernementales, conformément à la loi.

« Mobilité » des méthodes cryptographiques signifie uniquement la possibilité technique de fonctionner dans divers pays ou diverses infrastructures d'information et de communication.

« Non-répudiation » désigne une propriété obtenue par des méthodes cryptographiques, d'empêcher une personne ou une entité de nier avoir exécuté une action particulière en relation avec les données (par exemple mécanismes de non-répudiation d'origine; d'attestation d'obligation, d'intention ou d'engagement; ou d'établissement de la propriété).

« Données de caractère personnel » signifie toute information relative à une personne physique identifiée ou identifiable.

« Texte en clair » signifie des données intelligibles.

« Portabilité » des méthodes cryptographiques signifie la possibilité technique d'être adapté pour fonctionner sur de multiples systèmes.

IV. Intégration

Les principes contenus dans la section V de la présente Annexe, qui prennent chacun en compte un sujet de préoccupation majeur des pouvoirs publics, sont interdépendants et devraient être mis en œuvre comme un tout de manière à concilier les différents intérêts en jeu. Aucun principe ne devrait être mis en œuvre de façon isolée, indépendamment des autres.

V. Principes

1. Confiance dans les méthodes cryptographiques

Les méthodes cryptographiques devraient susciter la confiance afin que les utilisateurs puissent se fier aux systèmes d'information et de communication.

Les forces du marché devraient servir à créer la confiance dans des systèmes fiables, et les réglementations gouvernementales, la délivrance de licences et l'utilisation de méthodes cryptographiques pourraient également encourager la confiance des utilisateurs. L'évaluation des méthodes cryptographiques, en particulier par rapport à des critères acceptés par le marché, pourrait aussi contribuer à créer la confiance parmi les utilisateurs.

Pour promouvoir la confiance des utilisateurs, les contrats portant sur l'utilisation des systèmes de gestion des clés devraient indiquer le droit qui régit ces systèmes.

2. Choix des méthodes cryptographiques

Les utilisateurs devraient avoir le droit de choisir toute méthode cryptographique, dans le respect de la législation applicable.

Les utilisateurs devraient avoir un accès à la cryptographie qui réponde à leurs besoins, de telle manière qu'ils puissent avoir confiance dans la sécurité des systèmes d'information et de communication, et dans la confidentialité et l'intégrité des données sur ces systèmes. Les personnes ou entités qui possèdent, contrôlent, consultent, utilisent ou stockent des données peuvent avoir la responsabilité de préserver la confidentialité et l'intégrité de ces données, et peuvent donc avoir la responsabilité d'utiliser des méthodes cryptographiques appropriées. On peut penser que diverses méthodes cryptographiques seront peut-être nécessaires pour satisfaire les différentes exigences en matière de sécurité des données. Les utilisateurs de la cryptographie devraient être libres, dans le respect de la législation applicable, de déterminer le type et le niveau de sécurité requis des données, ainsi que de choisir et mettre en œuvre des méthodes cryptographiques appropriées, notamment un système de gestion de clés qui soit adapté à leurs besoins.

Pour protéger un intérêt public établi, comme la protection des données de caractère personnel ou le commerce électronique, les gouvernements peuvent mettre en œuvre des politiques qui imposent des méthodes cryptographiques afin d'assurer un niveau suffisant de protection.

Les mesures de contrôle gouvernemental sur les méthodes cryptographiques devraient se limiter à celles indispensables pour que les gouvernements s'acquittent de leurs responsabilités et devraient respecter dans toute la mesure du possible la liberté de choix des utilisateurs. Ce principe ne saurait être interprété comme impliquant que les gouvernements devraient préparer une législation qui limite le choix des utilisateurs.

3. Développement des méthodes cryptographiques guide par le marché

Les méthodes cryptographiques devraient être développées en réponse aux besoins, aux demandes et aux responsabilités des personnes, des entreprises et des gouvernements.

Le développement et l'offre de méthodes cryptographiques devraient être déterminés par le marché dans un environnement ouvert et concurrentiel. Une telle approche garantira au mieux que les solutions évolueront avec la technologie, les demandes des utilisateurs et les menaces pour la sécurité des systèmes d'information et de communication. Le développement des normes, critères et protocoles techniques internationaux sur lesquels s'appuient les méthodes cryptographiques devrait également être guidé par le marché. Les gouvernements devraient encourager les entreprises et la communauté de la recherche et coopérer avec elles dans le développement de méthodes cryptographiques.

4. Normes applicables aux méthodes cryptographiques

Des normes, critères et protocoles techniques applicables aux méthodes cryptographiques devraient être élaborés et instaurés aux échelons national et international.

Pour satisfaire les besoins du marché, les organismes de normalisation reconnus au plan international, les gouvernements et les entreprises de même que les autres experts compétents devraient mettre en commun l'information et collaborer pour élaborer et instaurer des normes, critères et protocoles techniques applicables aux méthodes cryptographiques qui assurent l'interopérabilité. Les éventuelles normes nationales applicables aux méthodes cryptographiques devraient être compatibles avec les normes internationales pour faciliter l'interopérabilité, la portabilité et la mobilité au plan mondial. Des mécanismes devraient être élaborés pour évaluer la conformité avec ces normes, critères et protocoles techniques relatifs à l'interopérabilité, à la portabilité et à la mobilité des méthodes cryptographiques. Dans la mesure où serait effectué un test de conformité aux normes, ou une évaluation de ces normes, il conviendrait d'encourager une large acceptation des résultats.

5. Protection de la vie privée et des données à caractère personnel

Les droits fondamentaux des individus au respect de leur vie privée, notamment au secret des communications et à la protection des données de caractère personnel, devraient être respectes dans les politiques nationales à l'égard de la cryptographie et dans la mise en œuvre et l'utilisation des méthodes cryptographiques.

Les méthodes cryptographiques peuvent être un instrument précieux pour protéger la vie privée, notamment en ce qui concerne tant la confidentialité des données et des communications que la protection de l'identité des personnes. Les méthodes cryptographiques offrent aussi de nouvelles possibilités de limiter le recueil de données de caractère personnel, en permettant des paiements, transactions et échanges sûrs mais anonymes. Dans le même temps, les méthodes cryptographiques destinées à assurer l'intégrité des données dans les transactions électroniques ont des implications sur le plan de la vie privée. Ces implications, notamment le recueil de données de caractère personnel et la création de systèmes d'identification des personnes, devraient être examinées et expliquées, et lorsqu'elles sont pertinentes des mesures de protection de la vie privée devraient être mises en place.

Les Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel fournissent des orientations générales concernant le recueil et la gestion des informations de caractère personnel, qui devraient être appliquées conjointement avec les dispositions pertinentes de la législation nationale lors de la mise en œuvre des méthodes cryptographiques.

6. Accès légal

Les politiques nationales à l'égard de la cryptographie peuvent autoriser l'accès légal au texte en clair ou aux clés cryptographiques de données chiffrées. Ces politiques doivent respecter dans toute la mesure du possible les autres principes énoncés dans les lignes directrices.

Lorsqu'ils envisagent des politiques relatives à des méthodes cryptographiques permettant un accès légal, les gouvernements devraient évaluer avec soin les avantages -- notamment en ce qui concerne la sécurité publique, le respect des lois et la sécurité nationale -- mais aussi les risques d'utilisation abusive, le surcoût des éventuelles infrastructures de soutien requises, les risques de défaillance technique, et les autres postes de dépenses. Ce principe ne saurait être interprété comme impliquant que les gouvernements devraient ou ne devraient pas promulguer une législation qui autoriserait l'accès légal.

Lorsque l'accès au texte en clair, ou aux clés cryptographiques, des données chiffrées est demandé en vertu de la procédure légale établie, la personne ou l'entité demandant cet accès doit être juridiquement habilitée à entrer en possession du texte en clair, et une fois les données obtenues celles-ci ne devraient être utilisées qu'à des fins licites. Le processus par lequel l'accès légal est obtenu devrait être consigné, afin que la divulgation des clés cryptographiques ou des données puisse être vérifiée ou examinée dans le respect des dispositions du droit national. Lorsqu'un accès légal est demandé et obtenu, cet accès devrait être accordé dans des délais prescrits adaptés aux circonstances. Les modalités de l'accès légal devraient être énoncées clairement, et publiées de telle manière qu'elles soient aisément disponibles pour les utilisateurs, détenteurs de clés et fournisseurs de méthodes cryptographiques.

Les systèmes de gestion de clés pourraient offrir une base pour une possible solution qui concilierait les intérêts des utilisateurs et ceux des organismes chargés de faire respecter la loi; ces techniques pourraient aussi servir à retrouver des données, en cas de perte des clés. Les procédures d'accès légal aux clés cryptographiques doivent tenir compte de la distinction entre les clés qui peuvent être utilisées pour protéger la confidentialité, et les clés qui sont utilisées exclusivement à d'autres fins. Une clé cryptographique qui uniquement donne l'identité ou assure l'intégrité (par opposition à une clé cryptographique qui uniquement vérifie l'identité ou l'intégrité) ne devrait pas être remise sans le consentement de la personne ou de l'entité en possession légale de cette clé.

7. Responsabilité

Qu'elle soit établie par contrat ou par voie législative, la responsabilité des personnes et entités qui proposent des services cryptographiques ou détiennent des clés cryptographiques ou y ont accès, devrait être clairement énoncée.

La responsabilité de toute personne ou entité, y compris une entité gouvernementale, qui offre des services cryptographiques, qui détient des clés cryptographiques ou qui a accès à des clés cryptographiques devrait être clairement énoncée, par contrat ou, le cas échéant, par la législation nationale ou par convention internationale. La responsabilité des utilisateurs en cas d'utilisation abusive de leurs propres clés devrait également être clairement énoncée. La responsabilité d'un détenteur de clés ne devrait pas pouvoir être engagée en cas de mise à disposition des clés ou du texte en clair des données chiffrées conformément à l'accès légal. La responsabilité de la partie qui obtient l'accès légal devrait pouvoir être engagée en cas d'utilisation abusive des clés cryptographiques ou du texte en clair qu'elle a obtenu.

8. Coopération internationale

Les gouvernements devraient coopérer en vue de coordonner les politiques à l'égard de la cryptographie. Dans le cadre de cet effort, les gouvernements devraient veiller à la levée, ou éviter de créer au nom de la politique de cryptographie, des obstacles injustifiés aux échanges.

Afin de promouvoir une large acceptation de la cryptographie au plan international et permettre aux réseaux d'information et de communication nationaux et mondiaux de se concrétiser pleinement, les politiques cryptographiques adoptées par un pays devraient être coordonnées autant que possible avec les politiques analogues adoptées par les autres pays. A cette fin, les Lignes directrices devraient être utilisées pour la formulation des politiques nationales.

S'ils sont développés, les systèmes nationaux de gestion de clés doivent, le cas échéant, permettre l'utilisation internationale de la cryptographie.

L'accès légal au-delà des frontières nationales pourra être réalisé par une coopération et des accords aux plans bilatéral et multilatéral.

Aucun gouvernement ne devrait empêcher la libre circulation de données chiffrées qui traversent sa juridiction du simple fait de sa politique de cryptographie.

Pour promouvoir les échanges internationaux, les gouvernements devraient éviter d'élaborer des politiques et pratiques de cryptographie qui créent des obstacles injustifiés au commerce électronique mondial. Les gouvernements devraient éviter d'entraver inutilement la disponibilité au plan international des méthodes cryptographiques.

Documents associés

RAPPORT SUR LA POLITIQUE DE CRYPTOGRAPHIE :
CONTEXTE ET QUESTIONS ACTUELLES[1]

Le Secrétariat a préparé ***ce rapport*** *sur le contexte et les questions actuelles de la politique de cryptographie pour expliquer le contexte dans lequel* ***les Lignes directrices*** *ont été établies et les questions de fond soulevées dans le débat sur la politique de cryptographie. Le rapport explique pourquoi une action internationale est nécessaire et il résume les travaux effectués à ce jour sur la question par l'OCDE et un certain nombre d'autres organisations. Il s'agit d'un document d'information qui a pour vocation de faciliter le débat public sur les Lignes directrices et non d'influer sur leur interprétation. Bien que donnant plus de détails sur l'éventail des questions couvertes par les Lignes directrices,* ***il ne modifie pas le sens de ces Lignes directrices et il ne doit pas servir de guide pour leur interprétation.*** *Ce rapport a été rédigé par le Secrétariat, qui s'est appuyé sur des discussions avec un certain nombre d'experts nationaux. Toutefois, il n'a été examiné que très brièvement lors des sessions plénières du Groupe ad hoc.*

I. GÉNÉRALITÉS

Évolution vers les transactions électroniques

L'information acquiert davantage de valeur et sa production, sa distribution et son utilisation représentent une activité économique de plus en plus importante. Elle s'échange souvent comme un produit de base, et elle peut être protégée au titre des dispositions sur la propriété intellectuelle. Les producteurs d'informations veulent avoir accès aux canaux de distribution, tandis que les consommateurs veulent pouvoir accéder à un large éventail de sources d'informations. De plus, la libre circulation de l'information est un élément fondamental de la démocratie.

Les systèmes traditionnels du téléphone, de la télévision hertzienne et par câble et de la radio font depuis longtemps appel à l'électronique pour diffuser l'information sous forme analogique ; le passage au numérique est en train de révolutionner la façon dont l'information est créée et stockée. Le traitement numérique sur ordinateur et les technologies de réseaux se substituent aux méthodes traditionnelles de production, de stockage, de transmission et de distribution de l'information. Il est aisé, avec la technologie numérique, de combiner différentes formes de représentation de l'information -- par exemple texte, son, image et vidéo -- et les distinctions entre les différentes formes de production et de distribution de l'information tendent à s'estomper. Par ailleurs, les nouveaux réseaux et les nouvelles technologies d'information et de communication sont en train de changer la façon dont les personnes communiquent et mènent des activités, et elles ont une profonde incidence sur les secteurs public et privé en imposant des changements dans diverses structures de base commerciales, juridiques ou autres.

La convergence de systèmes d'information et de communication auparavant distincts en un réseau mondial de réseaux crée des mécanismes pour réaliser de façon nouvelle des transactions, et elle va bientôt ouvrir un accès quasiment illimité à des sources d'information, d'enseignement et de loisirs. Cet accès s'accompagne aussi de nouveaux problèmes de propriété intellectuelle, propres à ce nouveau support. Si les réseaux d'information et de communication de type ouvert permettent de transmettre rapidement, économiquement et simplement, par des moyens électroniques, toutes les formes de données numérisées, la possibilité d'effectuer et de distribuer des copies parfaites de tous les types de données crée aussi un certain nombre de problèmes de protection de la propriété intellectuelle. Les échanges commerciaux de contenus créatifs peuvent générer des incitations

---

[1] Ce rapport a été rendu public en 1997 et n'a pas été mis à jour depuis. Les opinions exprimées et les arguments employés dans ce rapport ne reflètent pas nécessairement les vues officielles des Membres de l'OCDE.

économiques qui vont alimenter le développement des technologies d’information et de communication, et il est essentiel de protéger la propriété intellectuelle pour stimuler la production et les échanges de contenus de haute qualité.

Le commerce électronique offre des perspectives considérables pour les entreprises et les consommateurs, mais il s’accompagne aussi de quelques risques importants. La croissance mondiale explosive des réseaux ouverts a amené légitimement à s’interroger sur l’adéquation des mesures de sécurité et de protection de la vie privée dans les systèmes d’information et de communication et pour les données qui sont transmises et conservées sur ces systèmes. L’infrastructure de l’information qui se met en place constitue un environnement fertile pour toutes les formes de délinquance liées à l’informatique, y compris la fraude et les violations de la vie privée, et le commerce électronique ne pourra se développer tant que des mesures efficaces de sécurité des données n’auront pas été prises, dans lesquelles les utilisateurs et les consommateurs aient confiance. Des solutions tant techniques que juridiques doivent être trouvées pour rétablir dans le monde électronique la sécurité physique du monde sur papier. Il importe que les solutions choisies suscitent la confiance et que les consommateurs puissent s’y fier.

II. SÉCURITÉ DES SYSTÈMES D’INFORMATION ET CRYPTOGRAPHIE

Les systèmes d’information et de communication prennent de plus en plus d’importance pour la société et pour l’économie mondiale avec l’augmentation de la valeur et de la qualité des données qui sont transmises et stockées sur ces systèmes. Dans le même temps, ces systèmes et ces données sont de plus en plus vulnérables à diverses menaces, qu’il s’agisse de leur accès et leur utilisation sans autorisation, de leur détournement, de leur altération ou de leur destruction. La prolifération des ordinateurs, la montée en puissance des processeurs, l’interconnectivité, la décentralisation, l’expansion des réseaux et le nombre des utilisateurs, de même que la convergence des technologies de l’information et des communications, tout en renforçant l’utilité de ces systèmes, concourent aussi à leur vulnérabilité.

La sécurité des systèmes d’information et de communication consiste à protéger la disponibilité, la confidentialité et l’intégrité de ces systèmes et des données qui sont transmises et stockées sur ces systèmes. La disponibilité caractérise les systèmes d’information et de communication, l’information et les données qui sont accessibles et utilisables en temps voulu et de la manière requise. La confidentialité caractérise des données et des informations qui ne sont ni rendues disponibles ni divulguées aux personnes, entités ou mécanismes non autorisés. L’intégrité désigne des données et informations qui n’ont été ni modifiées ni altérées d’une manière non autorisée. La priorité relative et la signification de la disponibilité, la confidentialité et l’intégrité varient selon le système d’information ou de communication. La qualité de la sécurité des systèmes d’information et de communication et des données qui sont transmises et stockées sur ces systèmes dépend non seulement de mesures techniques, notamment de l’utilisation conjointe d’outils matériels et logiciels, mais aussi de l’application de bonnes procédures sur le plan de la gestion, de l’organisation et de l’exploitation.

La cryptographie est une composante importante dans la sécurité des systèmes d’information et de communication et un éventail d’applications ont été développées qui font appel à des méthodes cryptographiques pour assurer la sécurité des données. La cryptographie est un outil efficace pour assurer aussi bien la confidentialité que l’intégrité des données, et chacun de ces usages s’accompagne d’avantages particuliers. Cependant, l’usage généralisé de la cryptographie soulève un certain nombre de problèmes importants. Les gouvernements ont de vastes responsabilités et 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 électronique ; d’assurer la sécurité publique ; de lever des recettes pour financer leurs activités et de veiller au respect des lois et d’assurer la sécurité nationale. Bien qu’il existe, pour les gouvernements, les entreprises et les particuliers, des besoins et des usages légitimes de la cryptographie, celle-ci 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. Les gouvernements, en liaison avec l’industrie et le grand public, se doivent donc de dégager une politique qui concilie ces intérêts.

La diversité des intérêts qui peuvent être affectés par le fait d'utiliser, ou de ne pas utiliser, la cryptographie rend à la fois complexe et indispensable l'élaboration d'une politique équilibrée dans ce domaine. Traditionnellement, la cryptographie n'était le plus souvent utilisée que par les gouvernements. Ces dernières années, toutefois, la cryptographie devenant plus accessible et abordable et les utilisateurs devenant plus conscients des avantages liés à son utilisation et des risques attachés à sa non-utilisation, l'utilisation de la cryptographie en est venue à être considérée comme allant de soi par les particuliers et les entreprises dans un certain nombre d'applications. La cryptographie devenant de plus en plus accessible pour le grand public, le débat actuel sur ces questions s'en est trouvé lancé.

Cryptographie à clé secrète

Historiquement, la cryptographie servait à coder l'information de manière à rendre les messages secrets inaccessibles aux parties non autorisées et à ce titre elle est importante pour les applications liées à la défense et à la sécurité nationale. La cryptographie est basée sur l'utilisation d'un algorithme mathématique pour transformer des données, de manière à les rendre inintelligibles par quiconque ne possède pas certaines informations secrètes (la clé cryptographique) indispensables pour "déchiffrer" les données. Aujourd'hui, avec la puissance des moyens de calcul dont on dispose grâce à l'informatique numérique, il est possible d'utiliser des algorithmes mathématiques complexes pour chiffrer les données.

Avec le développement de technologies d'information et de communication permettant de transmettre, copier et stocker rapidement et aisément des volumes considérables de données, on se préoccupe de plus en plus de la protection de la vie privée et de la confidentialité des données, s'agissant notamment des données de caractère personnel, des dossiers de l'administration publique et des informations commerciales et financières. Des moyens cryptographiques efficaces apparaissent comme des outils essentiels dans un environnement de réseaux pour répondre à ces préoccupations. Ceux-ci servent aussi à protéger les informations gouvernementales classifiées.

Cryptographie à clé publique

Vers le milieu des années 70, grâce à une nouvelle avancée en cryptographie, est apparue le concept de "clé publique", qui permet à des parties d'échanger des données chiffrées sans avoir à se communiquer par avance une clé secrète commune. Au lieu de l'échange d'une seule clé secrète, ce nouveau système utilise deux clés mathématiquement liées pour chacune des parties à la communication : une clé publique, qui est révélée au public et qui sert à chiffrer les données, et une "clé privée" correspondante, qui est tenue secrète. Un message qui est chiffré avec une clé publique ne peut être déchiffré qu'avec la clé privée correspondante. Ainsi, une communication confidentielle chiffrée avec la clé publique du destinataire et déchiffrée avec la clé privée de celui-ci ne pourrait être comprise que par le destinataire du message[2].

Une application importante de la cryptographie à clé publique est celle des "signatures numériques", avec lesquelles on peut vérifier l'intégrité des données ou l'identité de leur expéditeur. En l'occurrence, la clé privée sert à signer le message, alors que la clé publique correspondante sert à vérifier le message signé. La cryptographie à clé publique offre en outre l'avantage de rendre confidentielles les transmissions et les signatures numériques dans un environnement de réseaux ouverts dans lequel les parties ne se connaissent pas à l'avance. Cette innovation a eu pour conséquence d'élargir l'éventail des applications des méthodes cryptographiques, évolution qui jointe à l'augmentation de la puissance et à la baisse des prix des ordinateurs a permis à la cryptographie de trouver des débouchés dans le secteur privé.

---

[2] Pour une description plus détaillée de la façon dont fonctionne la cryptographie à clé publique, voir :

"Cryptography's Role in Securing the Information Society", Computer Science and Telecommunications Board, United States National Research Council, National Academy Press, Washington, DC, 1996.

"Cryptography FAQ : Public Key Cryptography" ; Oxford University Libraries Automation Service, World Wide Web Server, www.lib.ox.ac.uk/internet/news/faq/archive/cryptography-faq.part06.html

"PUBLIC KEY CRYPTOGRAPHY", United States National Institute of Standards and Technology's Computer Security Resource Clearinghouse, NIST Special Publication 800-2, http://csrc.ncsl.nist.gov/nistpubs/800-2.txt.

La cryptographie à clé publique joue un rôle important dans le développement des infrastructures de l'information. Une bonne partie de l'intérêt porté aux réseaux et technologies d'information et de communication réside dans les possibilités qu'ils offrent pour le commerce électronique ; or des réseaux ouverts comme l'Internet soulèvent des problèmes non négligeables pour rendre exécutables les contrats électroniques et sécuriser les paiements. En liaison avec la certification de l'intégrité des données, la cryptographie à clé publique offre des solutions technologiques à ces deux types de problèmes en fournissant des mécanismes pour établir la validité de l'identité déclarée d'un utilisateur, d'un dispositif ou d'une autre entité au sein d'un système d'information ("authentification") et pour limiter les possibilités dont dispose une personne ou une entité de nier en pratique avoir effectué une action particulière concernant les données ("non-répudiation").

Signatures numériques

Les possibilités de fraude dans le monde électronique sont considérables. Les transactions s'effectuent à distance sans l'avantage des signes physiques permettant l'identification, ce qui facilite l'usurpation d'identité. La possibilité d'effectuer des copies parfaites et de modifier de façon indécelable les données numérisées rend la question encore plus complexe. Traditionnellement, on utilise les signatures manuscrites pour authentifier un document original. Dans le monde électronique, la notion de document "original" pose problème, mais une signature numérique peut servir à vérifier l'intégrité des données, et assurer une fonction d'authentification et de non-répudiation, vis-à-vis de l'expéditeur des données. Si le document lui-même a été modifié d'une quelconque façon après avoir été "signé", la signature numérique le révélera. De la même manière, dès lors qu'un document est signé au moyen d'une clé cryptographique, la signature numérique atteste que le document a été véritablement signé par l'auteur indiqué, et l'expéditeur ne peut aisément nier avoir envoyé le document ou prétendre que l'information a été modifiée en cours de transmission.

La cryptographie peut également fournir des solutions techniques pour protéger la propriété intellectuelle sous forme numérique. Ainsi, une signature numérique assortie d'un horodatage vérifiable peut donner aux auteurs un certain contrôle sur leurs oeuvres, en permettant d'établir un lien entre un document électronique et celui qui l'a diffusé et en garantissant que le document n'a pas subi de modifications qui ne soient décelables. La même technologie peut être mise en oeuvre pour assurer l'authenticité et l'intégrité des documents archivés électroniquement.

Paiements électroniques

Des systèmes de paiement sûrs sont également indispensables pour que le commerce électronique prenne son essor sur des réseaux ouverts. Un moyen pour effectuer des paiements électroniques serait d'utiliser une version aménagée du système actuellement en place pour les cartes de crédit. La cryptographie peut servir à protéger la confidentialité d'un message contenant un numéro de carte de crédit et pour confirmer que le message a bien été envoyé par le titulaire de la carte. Bien que cette méthode soit actuellement utilisée, le numéro de la carte de crédit reste vulnérable et peut être utilisé de façon inappropriée une fois décodé le message contenant le numéro. Une autre formule consiste à utiliser, pour que la transaction s'effectue électroniquement, des mécanismes de sécurité vérifiables qui ne soient pas simplement basés sur l'échange d'un numéro de carte de crédit, comme la confirmation indépendante par une signature numérique, conjugués à un processus d'autorisation qui ne soit pas lié à un réseau exclusif quelconque, de manière à rendre possibles les achats sur les réseaux ouverts.

Plusieurs systèmes basés sur d'autres formules de paiement électronique en sont à divers stades de développement, notamment un certain nombre de systèmes différents de "monnaie électronique". Ces systèmes de monnaie électronique reposent sur l'utilisation de la cryptographie pour créer une représentation électronique spécifique qui est remboursable ou qui peut avoir cours légal, et qui est stockable, transférable et infalsifiable. La plupart de ces systèmes fonctionnent dans une large mesure comme des cartes de crédit, des cartes de paiement ou des chèques, et ils offrent des possibilités plus ou moins développées de traçabilité et d'anonymat ; d'autres s'apparentent davantage à des "espèces électroniques", et permettent des transactions totalement anonymes, comme avec l'argent liquide. Bien que la possibilité d'effectuer des transactions électroniques intraçables et anonymes présente des avantages particuliers pour la protection de la vie privée dans un environnement électronique, elle suscite aussi un certain nombre de préoccupations chez les pouvoirs publics, notamment les autorités fiscales, en relation avec l'évasion fiscale et le blanchiment de capitaux.

Certification des relations en matières de clés publiques

L'affirmation de la relation entre une personne ou une entité et sa clé publique associée est importante pour prévenir les risques d'usurpation d'identité dans un environnement électronique. Pour que les systèmes à clés publiques fonctionnent dans le domaine public, il faut non seulement que les clés soient librement accessibles, mais aussi que les expéditeurs et les destinataires disposent d'un moyen fiable de s'assurer que les clés publiques sont véritablement celles des parties avec lesquelles ils souhaitent interagir. Cela est possible soit directement, si les parties se connaissent mutuellement à l'avance, soit par l'établissement d'un mécanisme officiel destiné à "certifier" les clés. Ainsi, deux types fondamentaux de solutions sont apparus : l'instauration d'un réseau informel de confiance, basé sur des relations préexistantes entre les parties, et une approche plus formalisée basée sur des "autorités de délivrance de certificats". Ces méthodes de certification des relations en matière de clés publiques fonctionnent dans une large mesure comme les moyens actuels utilisés pour l'identification des parties à l'occasion d'échanges sociaux ou commerciaux.

Le réseau informel de confiance intervient lorsque des clés sont validées de personne à personne ou d'organisation à organisation dans le contexte de relations établies. Ainsi, la confiance dans la relation entre un individu ou une entité et sa clé publique associée se transmet des parties en relation directe avec l'intéressé à celles qui ne le sont pas, la confiance se renforçant à mesure que se multiplient les exemples confirmant le crédit des intervenants. Cette méthode de certification des clés publiques est actuellement utilisée surtout pour l'échange de données chiffrées entre personnes se connaissant effectivement, mais avec le développement du commerce électronique, cette méthode pourrait évoluer pour devenir aussi un élément important des relations d'affaires.

L'autre catégorie fondamentale de solution pour traiter ce problème consiste en une infrastructure pour clés publiques dans laquelle des autorités de délivrance de certificats authentifient les clés publiques. Une autorité de délivrance de certificats est une entité "de confiance" qui fournit des informations sur l'identité du détenteur d'une clé sous la forme d'un "certificat de clé" authentifié. Le certificat sert à vérifier l'identité des parties qui échangent des informations chiffrées sur un réseau. Les autorités de délivrance de certificats peuvent aussi remplir d'autres fonctions, comme des services d'enregistrement notarial et d'horodatage. Elles peuvent être établies soit par le secteur public soit par le secteur privé, et peuvent fonctionner soit comme un service interne dans une organisation donnée soit comme un service proposé au public.

De plus, l'autorité de délivrance de certificats doit elle-même être fiable, de sorte qu'il faut que le certificateur puisse éventuellement être certifié. Cette question pourrait être résolue soit par une hiérarchie d'autorités de délivrance de certificats, soit par un système de certification mutuelle des autorités de délivrance de certificats. Au niveau international, des structures indépendantes pour la gestion internationale de la certification des clés publiques pourraient être utiles. La distinction entre le réseau de confiance et les méthodes basées sur les autorités de délivrance de certificats apparaît moins clairement quand les organisations qui assurent les fonctions de délivrance des certificats se certifient mutuellement. De nombreuses études ont montré que le commerce électronique ne prendra pleinement son essor que lorsque se mettront en place des infrastructures pour les clés publiques qui suscitent une confiance suffisante auprès des entreprises et des personnes pour que celles-ci acceptent de confier leurs informations et leurs transactions aux réseaux publics naissants. Rares sont les juridictions ayant d'ores et déjà adopté des législations spécifiques pour les infrastructures de certification ; un certain nombre de pays Membres étudient cette question et envisagent des procédures de réglementation et d'autorisation applicables aux autorités de délivrance de certificats.

III. QUESTIONS SPECIFIQUES A CONSIDERER DANS LE CADRE DE LA POLITIQUE DE CRYPTOGRAPHIE

Confiance des utilisateurs

De plus en plus, les particuliers, les entreprises et les gouvernements subissent l'influence des systèmes électroniques d'information et de communication, et ils constatent qu'ils sont de plus en plus tributaires du fonctionnement adéquat et ininterrompu de ces systèmes. Parallèlement, ils éprouvent de plus en plus le besoin de pouvoir penser que ces systèmes demeureront fiables et sûrs, compte tenu notamment du développement des systèmes de commerce électronique et de paiement électronique. L’absence de sécurité ou de confiance dans la sécurité de ces systèmes pourrait freiner le développement et l’utilisation des nouvelles technologies d’information et de communication.

Tout comme dans le monde réel, où les cartes de crédit se falsifient et où l’argent se vole, le “monde virtuel” ne sera jamais totalement sûr. Il faut certes que les méthodes et les services de sécurité suscitent la confiance, pour que les utilisateurs des systèmes d’information et de communication puissent s’y fier, mais en définitive les transactions électroniques impliqueront un risque calculé. Les consommateurs opteront pour le commerce électronique lorsque l’intérêt qu’il présente l’emportera sur les risques apparents. La question qui se pose n’est donc plus de savoir si les transactions sont absolument sûres, mais si elles apparaissent suffisamment sûres pour les transactions des consommateurs ? Il importe de consolider la confiance des consommateurs dans les mécanismes de sécurité des données, comme la cryptographie, afin que ceux-ci soient largement utilisés pour le commerce électronique.

Il est possible de lever les incertitudes et d’encourager la confiance en forgeant un consensus sur l’utilisation des systèmes d’information et de communication. Le défi est triple : développer et mettre en place la technologie ; se préparer pour éviter les défaillances de la technologie et y faire face ; et gagner le soutien du public et son adhésion à l’utilisation de la technologie. L’éducation du public sur les questions posées et sur les technologies, notamment une discussion approfondie de la cryptographie dans le contexte du commerce électronique, pourrait contribuer à renforcer la confiance des consommateurs. Dans ce contexte, il est également important que les utilisateurs comprennent le cadre juridique qui régit leur usage de la cryptographie, compte tenu notamment du caractère “sans frontière” des réseaux d’information et de communication.

Choix des utilisateurs

Les solutions visant à protéger contre les diverses menaces à l’égard des systèmes d’information et de communication et des données qui sont stockées et transmises sur ces réseaux peuvent prendre diverses formes. Il existe un choix considérable de méthodes cryptographiques disponibles pour satisfaire un très large éventail de besoins des utilisateurs en matière de sécurité des systèmes et des données, notamment des solutions tant matérielles que logicielles, qui peuvent être indépendantes ou intégrées dans des produits connexes, et qui offrent un certain niveau de robustesse et de complexité en fonction de l’algorithme et du produit. Les méthodes cryptographiques peuvent être conçues de manière à combiner n’importe quels mécanismes pour assurer la confidentialité, l’authentification ou la non-répudiation ainsi que l’intégrité des données. Les utilisateurs choisiront différents types de méthodes cryptographiques pour différents usages et pour répondre à différents besoins en matière de sécurité des données et des systèmes. De plus, dans les cas où des systèmes de gestion de clés seront mis en place, ceux-ci offriront aussi diverses fonctions entre lesquelles les utilisateurs choisiront.

Certains gouvernements ont introduit des réglementations, et d’autres pourraient le faire à l’avenir, concernant l’utilisation de la cryptographie, notamment des contrôles à l’exportation, des règles concernant les systèmes de gestion de clés ou des obligations quant aux niveaux minimaux de protection de certaines catégories de données. Ces réglementations pourraient avoir une incidence sur les types de méthodes cryptographiques disponibles et entre lesquelles les utilisateurs peuvent choisir. On s’accorde toutefois à reconnaître que, malgré ces limitations, il est important qu’un large éventail de méthodes cryptographiques soit disponible pour répondre à la diversité des besoins en matière de sécurité des données et des systèmes. La diversité des options dans le choix des méthodes cryptographiques encouragera la mise au point d’un large éventail de produits.

Développement guidé par le marché

Puisque le secteur privé est un partenaire essentiel dans l’édification de l’infrastructure d’information, et qu’il a la responsabilité première de sa construction, la plupart des experts s’accordent sur le fait que c’est à l’industrie de développer des produits et de déterminer les normes sur la base des besoins du marché. S’il est admis que les gouvernements puissent influencer le développement des produits en exprimant, comme tout utilisateur, le besoin d’un certain type de produit, certains considèrent que les gouvernements devraient veiller à ne pas conduire les marchés dans une direction donnée. D'autres estiment que les gouvernements devraient guider le marché pour remplir leurs responsabilités en matière de protection de la sécurité publique et de la vie privée. Néanmoins, les gouvernements sont aussi conscients du fait que si les obligations qu'ils imposent sur l'utilisation de la cryptographie sont trop lourdes, les utilisateurs des systèmes d'information et de communication n'utiliseront pas la cryptographie, et l'industrie ne développera pas de produits faisant appel aux techniques cryptographiques.

Normalisation

La normalisation est une composante importante des mécanismes de sécurité. Avec le développement rapide de l'infrastructure de l'information, des normes pour les mécanismes de sécurité, notamment des méthodes cryptographiques, se dégagent rapidement, qu'elles soient de facto, par la domination sur le marché, ou qu'elles soient issues des organismes de normalisation nationaux ou internationaux. Il importe que les gouvernements et les entreprises oeuvrent ensemble pour établir l'architecture et les normes nécessaires afin que les systèmes d'information et de communication puissent tenir toutes leurs promesses. On s'accorde à considérer qu'un processus efficace de normalisation est un processus piloté par l'industrie, de caractère volontaire, basé sur le consensus et à vocation internationale.

Pour que la cryptographie puisse être utilisée en pratique comme un moyen de sécurité pour les systèmes, réseaux et infrastructures d'information et de communication, il est important que les méthodes cryptographiques soient interopérables, mobiles et portables à l'échelle mondiale. L'interopérabilité désigne la capacité pour de multiples méthodes cryptographiques de techniquement fonctionner ensemble. La mobilité désigne la capacité technique permettant à des méthodes cryptographiques de fonctionner dans de multiples infrastructures d'information et de communication. La portabilité désigne la possibilité technique pour des méthodes cryptographiques d'être adaptées pour fonctionner sur de multiples systèmes. Des normes nationales et internationales applicables aux méthodes cryptographiques peuvent contribuer à faciliter le développement de ces capacités techniques.

Protection de la vie privée

Le respect de la vie privée et la confidentialité des données de caractère personnel sont des valeurs importantes dans une société démocratique. Pourtant, la vie privée est aujourd'hui davantage menacée dans l'infrastructure de l'information et des communications qui se met en place car ni les réseaux ouverts, ni les nombreux types de réseaux privés ont été conçus en ayant à l'esprit la confidentialité des communications et du stockage des données. Toutefois, la cryptographie constitue la base d'une nouvelle génération de technologies susceptibles de contribuer à renforcer le respect de la vie privée. L'utilisation d'une cryptographie efficace dans un environnement de réseau peut aider à protéger la confidentialité des informations de caractère personnel et le secret des informations confidentielles. Le fait de ne pas utiliser la cryptographie dans un environnement où les données ne sont pas complètement sûres peut nuire à certains intérêts, notamment à la sécurité publique et à la sécurité nationale. Dans certains cas, en particulier lorsque la législation impose la garantie de la confidentialité des données ou la protection d'infrastructures essentielles, les gouvernements peuvent demander l'emploi d'une cryptographie offrant une robustesse minimale.

Dans le même temps, l'utilisation de la cryptographie pour assurer l'intégrité des données dans les transactions électroniques peut avoir des implications au plan de la vie privée. L'usage des réseaux pour toutes les formes de transactions va de plus en plus générer des volumes énormes de données qui peuvent être facilement et au moindre coût stockées, analysées et réutilisées. Lorsque ces transactions impliquent une preuve d'identité, ces données transactionnelles conserveront les traces détaillées et éventuellement irréfutables des activités commerciales d'une personne, en même temps qu'elles dessineront une image de ses activités privées non commerciales, comme ses appartenances politiques, sa participation à des discussions en ligne, et ses consultations de catégories spécifiques d'informations dans des bibliothèques en ligne ou dans d'autres banques de données. La procédure de certification des clés a aussi des implications pour la vie privée, car des données peuvent être recueillies lorsqu'une autorité de certification établit un lien entre une personne et une paire de clés.

Accès légal

Une question essentielle soulevée par la cryptographie -- sans doute l'aspect le plus débattu de la cryptographie et celui qui est le plus susceptible de conduire à des politiques nationales hétérogènes -- est l'opposition apparente entre confidentialité et sécurité publique. Bien que l'utilisation de la cryptographie soit importante pour la protection de la vie privée, il semblerait nécessaire de considérer des mécanismes qui permettent l'accès légal à l'information chiffrée. Ainsi, dans de nombreux pays, les autorités compétentes peuvent légalement accéder aux données conservées en mémoire ou intercepter les communications (ou les deux), sous certaines conditions. Ces deux importants moyens de faire respecter la loi pourraient être vidés de leur substance par une utilisation de la cryptographie qui pourrait empêcher l'accès légal soit au texte en clair soit aux clés cryptographiques de données chiffrées. Dans certains cas, le chiffrement de données conservées en mémoire peut rendre impossible leur accès par les autorités compétentes, tandis que dans d'autres cas il serait légalement possible d'accéder ailleurs aux données (par exemple obtention des relevés financiers auprès de la banque, plutôt que sur l'ordinateur personnel de l'intéressé), ou d'obtenir les clés pour déchiffrer les données. Pour les pays qui autorisent l'une ou l'autre de ces techniques, l'arbitrage entre les considérations de protection de la vie privée et de la confidentialité des informations économiques et celles liées à la protection de la sécurité publique et de la sécurité nationale est politiquement ardu.

En outre, le besoin d'accès par des tiers ne se limite pas aux pouvoirs publics. Des personnes privées et des entreprises peuvent aussi avoir besoin d'accéder à des informations chiffrées. On peut prendre ainsi l'exemple d'une personne qui décède en laissant des informations chiffrées sans la clé pour les déchiffrer, ou celui d'un employé qui a chiffré un fichier et démissionne sans laisser d'information sur la clé de déchiffrement. Les particuliers et les entreprises qui chiffrent des données peuvent souhaiter placer une copie de leurs clés cryptographiques en dépôt, ce qui dans les cas précédemment mentionnés permettrait un accès légal aux informations.

Il importe de noter la différence entre les clés cryptographiques utilisées à des fins de confidentialité et celles utilisées uniquement pour l'authentification, l'intégrité des données et la non-répudiation. Le problème de l'accès légal aux clés cryptographiques se pose plutôt pour les utilisations de la cryptographie qui ont pour objet de garder confidentielles des données, lorsque celles-ci sont dissimulées. La cryptographie utilisée à la seule fin d'authentifier ou d'assurer l'intégrité des données ne dissimule pas nécessairement l'information ; elle vérifie seulement les données. Dans ces circonstances, les données elles-mêmes peuvent déjà être disponibles, ou elles pourraient être légalement obtenues par d'autres voies, de sorte qu'il serait inutile d'avoir accès à la clé privée. Une conséquence importante de l'utilisation de clés privées uniquement pour l'authentification ou la garantie de l'intégrité des données est que lorsqu'une telle clé est compromise, il existe un risque d'usurpation d'identité électronique. Comme les clés publiques sont généralement conçues pour être mises dans le domaine public, ces questions ne concernent généralement pas l'accès aux clés publiques.

Si l'accès légal doit être préservé, la façon précise de procéder n'apparaît pas clairement. Les gouvernements poursuivent des approches différentes et recherchent des solutions novatrices auprès de l'industrie. Une approche qui pourrait servir de base à une possible solution pour concilier les intérêts des utilisateurs et ceux des autorités chargés de faire appliquer la loi consisterait à utiliser un système de gestion de clés dans lequel une copie de la clé cryptographique privée utilisée à des fins de confidentialité serait “conservée” par une “tierce partie de confiance” (TPC)3. D'autres approches permettraient de donner à des tiers un accès légal au texte clair correspondant aux données chiffrées. Parmi l'ensemble des approches possibles, certaines pourraient également servir à récupérer les données en cas de perte des clés. Rappelons qu'il est important de bien voir la distinction entre les clés utilisées pour protéger la confidentialité et celles utilisées à d'autres fins uniquement. Les clés utilisées

---

3. Une TPC est un tiers indépendant, appartenant soit au secteur public soit au secteur privé, qui fournit des services sécurisés pour les réseaux d'information et de communication. En l'occurrence, les services sécurisés de la TPC consisterait à conserver la clé selon certaines modalités et conditions, et en accord avec les parties intéressées. Dans un tel système, les clés, ou le texte en clair des données chiffrées, le cas échéant, pourraient être accessibles en vertu d'un pouvoir légal, mandat légal ou décision judiciaire par exemple, délivré par l'autorité compétente.

pour l'authentification, la vérification de l'intégrité des données et la non-répudiation ne seraient pas soumises aux mêmes types d'accès légal par des tiers.

Dans ce contexte, un certain nombre d'autres problèmes devraient peut-être être résolus, notamment ceux de savoir où les clés seront conservées, qui sera autorisé à détenir des clés, et quelles seront les responsabilités et obligations des détenteurs de clés. Ces systèmes de stockage de clés sont indépendants des infrastructures de clés publiques pour la certification des clés publiques -- autre forme de service sécurisé que pourrait fournir une TPC -- bien que les deux services puissent être combinés.

Responsabilité

Comme de nombreuses choses dans la vie, les technologies de l'information et des communications ne fonctionnent pas toujours parfaitement : les pare-feux ne parviennent pas à tenir à distance les intrus, les réseaux peuvent tomber en panne, les routeurs peuvent se tromper de destination en expédiant les données. A cela peut venir s'ajouter l'erreur humaine, par exemple lorsque des données sont effacées par erreur ou que des mots de passe ne sont pas gardés secrets. Dans le contexte de la cryptographie, une défaillance de système ou une erreur humaine aboutissant à la divulgation de clés cryptographiques peut avoir de lourdes conséquences, car la plus robuste des cryptographies devient inefficace si les clés sont révélées. Lorsque tel est le cas, les utilisateurs doivent considérer que leurs données chiffrées ne sont plus sûres, et ils courent le risque que des documents ou transactions soient falsifiés avec leur nom. Lorsque la sécurité d'une autorité de délivrance de certificats est compromise, les conséquences peuvent être catastrophiques. De plus, le processus de révocation des clés et des certificats de clés peut être complexe.

Il est très important que les clés soient gérées de façon sûre, aussi bien pour les utilisateurs individuels que pour les organisations : les systèmes de gestion de clés prévoient généralement des procédures strictes pour protéger et surveiller l'utilisation des clés, afin d'éviter qu'elles ne soient révélées. Toutefois, si ces pratiques échouent et les clés deviennent connues, il est important de savoir quelles sont les parties qui doivent en assumer la responsabilité et dans quelle mesure leur responsabilité est engagée pour ce qui est des conséquences qui en résultent. Cette question est particulièrement importante pour les services de gestion de clés ou les tiers de confiance, qui détiennent des clés cryptographiques ou y ont accès pour le compte d'autrui, étant donné les conséquences au plan de la responsabilité civile en cas de violation de la sécurité de leur système. La définition des dispositions applicables en matière de responsabilité peut se faire par voie soit contractuelle soit législative, au niveau des personnes ou des gouvernements. De plus, il importerait peut-être d'examiner les implications en matière de responsabilité aux plans tant national qu'international.

Coopération internationale

Le caractère de plus en plus planétaire des flux de données sur les réseaux d'information et de communication fait ressortir la nécessité d'une approche internationale en coopération pour l'examen de ces questions. L'application des régimes juridiques en place s'organise à l'intérieur de frontières géographiquement définies, alors que dans le nouvel environnement de réseau qui apparaît, les informations et les transactions commerciales peuvent circuler librement à travers les frontières nationales et juridictionnelles. En élaborant leurs stratégies nationales et en concevant des structures réglementaires pour les infrastructures de l'information, notamment celles touchant la cryptographie, tous les gouvernements en viennent à reconnaître que dans de nombreux cas, ces activités auront des incidences qui s'étendront bien au-delà de leurs frontières.

Les disparités des politiques nationales pourraient freiner le développement des réseaux et technologies à l'échelle mondiale, en imposant l'utilisation de nombreux produits, peut-être incompatibles, pour communiquer et réaliser des transactions commerciales alors qu'un seul pourrait suffire. Un tel environnement pourrait également créer des barrières aux échanges internationaux. Étant donné le caractère intrinsèquement mondial des réseaux d'information et de communication qui se mettent en place et les difficultés rencontrées pour définir et faire appliquer les frontières juridictionnelles dans cet environnement, la façon peut-être la plus efficace d'aborder ces questions serait d'agir par le biais de consultations et de coopérations internationales. Une telle approche est particulièrement pertinente dans le cas de la cryptographie.

IV. ACTIVITÉS GOUVERNEMENTALES LIÉES À LA POLITIQUE DE CRYPTOGRAPHIE

Activités à l'échelon national

De nombreux pays Membres de l'OCDE se sont engagés dans l'élaboration de lois et réglementations sur la cryptographie au milieu des années 90. Les politiques nationales ont toutefois commencé à être développées indépendamment les unes des autres, et il est rapidement apparu que les disparités sur le plan du droit pouvaient susciter des obstacles au développement des réseaux d'information et de communication nationaux et mondiaux. Lorsque l'OCDE a été invitée à examiner la question de la politique de cryptographie en 1995, plusieurs pays Membres de l'OCDE disposaient déjà de textes législatifs qui prenaient en compte certains aspects de la politique de cryptographie (notamment signatures numériques et réglementations d'exportation). Beaucoup d'autres pays avaient des initiatives législatives en attente ou étudiaient les problèmes en vue d'élaborer une législation. Ces efforts conduits au plan national et l'expérience des situations nationales que les délégations ont apportés à la table de rédaction à l'OCDE ont contribué à éclairer les problèmes et les implications de la politique de cryptographie et ils ont fourni une base solide pour une coopération internationale dans ce domaine.

La politique de cryptographie à l'OCDE

L'OCDE est un lieu d'échanges privilégié pour passer en revue les questions d'intérêt commun en ce qui concerne la politique de cryptographie, car elle a l'habitude d'aborder les questions de politique générale combinant différents aspects touchant l'économie, la technologie et le droit, et de développer la prise de conscience et le consensus au plan international sur les questions liées à la sécurité des systèmes d'information, à la protection des données de caractère personnel et de la vie privée et aux technologies de l'information, de l'informatique et des communications. L'OCDE a déjà, par le passé, servi de lieu de discussion sur les technologies de cryptographie et les questions socio-économiques soulevées par l'utilisation de la cryptographie.

Les *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel de l'OCDE,* de 1980, comme les *Lignes directrices régissant la sécurité des systèmes d'information de l'OCDE,* de 1992, ont mis en évidence le besoin de moyens techniques pour assurer la protection des données personnelles et de la vie privée ainsi que la sécurité des systèmes d'information. Depuis 1989, le Comité de la politique de l'information, de l'informatique et des communications (PIIC) de l'OCDE a inclus les technologies et politiques de cryptographie dans ses travaux sur la sécurité et la vie privée. Dans un rapport de 1989 du Secrétariat de l'OCDE intitulé *La sécurité des réseaux informatiques*, figure une analyse des questions liées aux technologies et politiques de cryptographie, questions qui ont également été examinées à la Réunion sur la sécurité de l'information de l'OCDE, en mars 1990. C'est à la réunion d'experts sur les évolutions récentes dans le domaine de la protection des données de caractère personnel et de la vie privée, tenue les 10 et 11 décembre 1992, que les technologies et politiques de cryptographie ont été pour la première fois examinées de façon approfondie dans une réunion de l'OCDE. Au cours de cette réunion, des orateurs du secteur privé et du monde universitaire ont présenté la cryptographie, décrit différentes technologies et débattu des questions posées au plan de l'action gouvernementale. De même, lors de la Réunion d'experts sur les Infrastructures de l'information, qui a eu lieu à l'OCDE du 30 novembre au 2 décembre 1994, une session a été consacrée à la politique de cryptographie. Les participants ont souligné les liens entre la politique de cryptographie, la protection des données de caractère personnel et de la vie privée, la sécurité des systèmes d'information et la protection de la propriété intellectuelle, et ils ont insisté sur le fait que la poursuite des objectifs de sécurité et de protection de la vie privée et de la propriété intellectuelle doit se faire de façon équilibrée, de telle manière que les solutions introduites dans un domaine n'aient pas d'effet préjudiciable sur un autre plan, ou ne créent pas des obstacles injustifiés aux échanges.

La Réunion ad hoc d'experts sur la politique de cryptographie organisée par l'OCDE les 18 et 19 décembre 1995 a focalisé l'attention sur ces questions et donné aux pays Membres une possibilité de comparer leurs positions nationales sur la politique de cryptographie et d'en débattre. Participaient à cette réunion divers groupes de représentants des pouvoirs publics -- notamment des représentants des ministères du commerce, de l'industrie et des télécommunications, des services responsables de la protection des données et des organismes chargés de faire respecter les lois et d'assurer la sécurité nationale -- ainsi que des membres du secteur privé, dont un grand nombre d'experts techniques. Le débat a fait ressortir le besoin de solutions nationales compatibles et harmonisées au plan international, qui concilient de façon appropriée les impératifs en matière de protection des données et ceux liés au respect des lois.

Le secteur privé a joué un rôle important dans l'élaboration de lignes directrices sur une politique de cryptographie à l'OCDE. Conformément au mandat donné lors de la réunion de 1995 du Conseil de l'OCDE au niveau des Ministres selon lequel il convenait d'associer aux travaux sur l'infrastructure mondiale de l'information des partenaires non-gouvernementaux, un Forum gouvernements-secteur privé sur une politique mondiale de cryptographie a été organisé conjointement par la CCI (Chambre de commerce internationale), le BIAC et l'OCDE les 19 et 20 décembre 1995, à l'occasion de la réunion ad hoc. Lors de ce Forum, le secteur privé a pu exposer son point de vue et présenter un certain nombre d'initiatives d'entreprises pour une politique mondiale en matière de cryptographie.

Le Groupe d'experts de l'OCDE sur la sécurité, la vie privée et la protection de la propriété intellectuelle dans l'infrastructure mondiale de l'information, qui s'est réuni pour la première fois à Canberra (Australie) le 9 février 1996, a approuvé la proposition des États-Unis tendant à ce que l'OCDE prépare des Lignes directrices sur la politique de cryptographie. A la 29ème session du Comité PIIC tenue les 27-29 mars 1996, le Groupe ad hoc d'experts sur les Lignes directrices régissant la politique de cryptographie a été constitué.

Le Communiqué qui a été diffusé à l'issue de la réunion des 21 et 22 mai 1996 du Conseil de l'OCDE au niveau des Ministres mentionnait explicitement la politique de cryptographie dans ses orientations des travaux de l'Organisation :

> "15. Pour faciliter la mise en œuvre de leurs engagements, compte tenu de la nécessité de réaliser les nouveaux travaux avec un budget restreint, en se concentrant sur les grandes priorités, les Ministres donnent à l'OCDE le mandat suivant :
>
> (iv) Approfondir ses travaux sur un cadre d'action global en vue de faciliter le développement de l'infrastructure mondiale de l'information et des produits et services qui lui sont reliés, et notamment l'établissement de lignes directrices en matière de chiffrement qui permettraient d'améliorer la sécurité et de protéger les droits de propriété intellectuelle dans ce domaine, et analyser les incidences économiques et sociales ; ".

Alors que ces questions prenaient de l'importance dans l'opinion publique, le processus d'élaboration des Lignes directrices a officiellement débuté avec la première réunion du Groupe ad hoc d'experts, qui s'est tenue à Washington, D.C. le 8 mai 1996. Un deuxième Forum gouvernements-secteur privé sur la politique mondiale de cryptographie, organisé conjointement par la CCI, le BIAC et l'OCDE le 7 mai 1996, a donné aux membres du Groupe ad hoc une nouvelle occasion de débattre de ces questions avec des représentants du secteur privé. Les travaux se sont poursuivis tout au long de l'année avec trois autres réunions du Groupe en juin, en septembre et en décembre 1996. Avant la réunion de septembre, des membres du Groupe ad hoc ont participé à un colloque public, organisé par l'Electronic Privacy Information Center, qui a permis d'entendre les points de vue d'éminents spécialistes de la cryptographie, experts techniques et défenseurs des droits de la personne humaine sur les évolutions récentes concernant la politique de cryptographie. Plus d'une centaine de délégués représentant les gouvernements, le secteur privé et les groupes de défense des utilisateurs ont assisté à chacune des réunions du Groupe ad hoc.

À sa deuxième réunion des 27 et 28 janvier 1997, le Groupe d'experts sur la sécurité, la vie privée et la protection de la propriété intellectuelle dans l'infrastructure mondiale de l'information a examiné et approuvé le projet de Lignes directrices. Le Comité PIIC a entériné le projet de Lignes directrices à sa réunion des 27 et 28 février 1997, et a transmis le document au Conseil. Le Conseil a adopté les Lignes directrices en tant que Recommandation du Conseil relative aux Lignes directrices régissant la politique de cryptographie le 27 mars 1997.

Autres travaux liés à la politique de cryptographie à l'échelon national et international

Des législations sur la protection des données et le respect de la vie privée sont en vigueur dans un certain nombre de pays et dans l'Union européenne depuis quelques années. 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, par exemple, impose la mise en oeuvre de mesures techniques et organisationnelles appropriées pour protéger les données de caractère personnel contre les risques de destruction accidentelle, d'altération, ou de divulgation ou d'accès non autorisé, notamment dans le cas de données transmises sur un réseau. Cette Directive soulève des problèmes spécifiques dans le débat sur la politique de cryptographie, car la cryptographie est un moyen important d'assurer la confidentialité des données.

Les produits et technologies faisant appel à la cryptographie ont de tout temps fait l'objet de contrôles à l'exportation. La base actuelle des contrôles à l'exportation est l'Arrangement de Wassenaar sur les contrôles à l'exportation des armes conventionnelles et des biens et technologies à double usage (convenu le 13 juillet 1996), dont les listes de contrôle à l'exportation couvrent les produits cryptographiques. Cet Arrangement a été transposé dans les réglementations nationales. 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 s'appliquent également à l'exportation de produits cryptographiques. Quelques États ont imposé à titre isolé d'autres contrôles spécifiques sur cette catégorie d'exportations, qui continuent de faire l'objet d'un débat.

Le Conseil de l'Europe a consacré des ressources considérables à l'étude de la question de la criminalité informatique, avec notamment la diffusion de la Recommandation [R(95)13] du Conseil de l'Europe en date du 11 septembre 1995 relative aux problèmes de procédure pénale liés à la technologie de l'information, et il envisage de proposer une convention internationale pour s'attaquer à ce problème. Cette convention aborderait des questions comme l'échange d'informations entre organismes gouvernementaux dans les affaires faisant intervenir l'utilisation de la cryptographie.

Lors du Sommet du G-7 sur l'anti-terrorisme tenu en juillet 1996, les Gouvernements du G-7 ont annoncé que les consultations seraient accélérées “dans les instances bilatérales et multilatérales appropriées sur le cryptage des informations permettant, si nécessaire, l'accès légal des gouvernements aux données et communications afin, notamment, de lutter contre et enquêter sur les actes de terrorisme, tout en protégeant le caractère privé des communications légitimes”.

En mai 1996, le CSTB (Computer Science and Telecommunications Board) du Conseil national de la recherche des États-Unis a publié un rapport intitulé “Cryptography's Role in Securing the Information Society”. Cette étude interdépartementale évalue les effets pour les États-Unis des technologies cryptographiques sur la sécurité nationale, le respect des lois et les intérêts des entreprises et des particuliers, et elle passe en revue l'incidence des contrôles à l'exportation sur les technologies cryptographiques. Ce rapport qui fait autorité présente un tour d'horizon complet des questions de politique de cryptographie auxquelles le Gouvernement des États-Unis doit faire face.

Aucun de ces efforts, toutefois, n'a visé à envisager dans son ensemble la question de la politique internationale de cryptographie, ou à identifier les divers intérêts qui doivent être conciliés de façon équilibrée dans le contexte d'une politique internationale de cryptographie. Dans ce domaine, les Lignes directrices de l'OCDE régissant la politique de cryptographie ont pour vocation d'aider les pays Membres en portant ces questions à leur attention.

V. AUTRES QUESTIONS

Pays non membres

La Recommandation s'adresse aux pays Membres. Il est toutefois souhaitable que l'existence des Lignes directrices soit plus largement reconnue, et les pays non membres devraient être encouragés à souscrire à la Recommandation. Compte tenu du développement des réseaux d'information et de communication mondiaux et de la nécessité de garantir l'adoption de solutions concertées, on s'attachera à porter les Lignes directrices à l'attention des pays non membres et des organisations internationales compétentes en la matière.

Le contexte général

Compte tenu du rôle de la cryptographie dans l'infrastructure de l'information et des communications et dans le développement du commerce électronique, la politique en la matière empiète sur les aspects économiques, juridiques et politiques d'un certain nombre de domaines voisins, notamment la sécurité des systèmes d'information, la protection de la vie privée et des données de caractère personnel, et la protection de la propriété intellectuelle. Pour que les réseaux et les technologies d'information et de communication tiennent toutes leurs promesses, les gouvernements nationaux devraient se pencher sur les questions liées à la cryptographie qui empêchent un commerce électronique sûr, notamment l'absence de normes et le rôle des autorités de certification.

Aux termes de son mandat, le Groupe ad hoc avait pour mission d'élaborer des lignes directrices sur les questions fondamentales à prendre en considération dans l'élaboration de la politique de cryptographie. Les Lignes directrices sont un instrument nouveau s'ajoutant aux instruments internationaux existants qui régissent des questions telles que les droits de la personne humaine, les échanges internationaux, le copyright et les droits d'auteur, les télécommunications et divers services d'information. Si le besoin s'en faisait sentir, il serait possible dans le cadre des activités entreprises par l'OCDE dans le domaine des politiques de l'information, de l'informatique et des communications, d'approfondir encore les principes énoncés dans les Lignes directrices.

À propos de l’OCDE

L’OCDE est un forum unique en son genre où les gouvernements œuvrent ensemble pour relever les défis économiques, sociaux et environnementaux que pose la mondialisation. L’OCDE est aussi à l’avant- garde des efforts entrepris pour comprendre les évolutions du monde actuel et les préoccupations qu’elles font naître. Elle aide les gouvernements à faire face à des situations nouvelles en examinant des thèmes tels que le gouvernement d’entreprise, l’économie de l’information et les défis posés par le vieillissement de la population. L’Organisation offre aux gouvernements un cadre leur permettant de comparer leurs expériences en matière de politiques, de chercher des réponses à des problèmes communs, d’identifier les bonnes pratiques et de travailler à la coordination des politiques nationales et internationales.

Les pays Membres de l’OCDE sont : l’Allemagne, l’Australie, l’Autriche, la Belgique, le Canada, le Chili, la Colombie, la Corée, le Costa Rica, le Danemark, l’Espagne, l’Estonie, les États Unis, la Finlande, la France, la Grèce, la Hongrie, l’Irlande, l’Islande, Israël, l’Italie, le Japon, la Lettonie, la Lituanie, le Luxembourg, le Mexique, la Norvège, la Nouvelle Zélande, les Pays Bas, la Pologne, le Portugal, la République slovaque, la République tchèque, le Royaume-Uni, la Slovénie, la Suède, la Suisse et la Türkiye. L’Union européenne participe aux travaux de l’OCDE.

Instruments juridiques de l’OCDE

Environ 460 instruments juridiques de substance ont été développés dans le cadre de l’OCDE depuis sa création en 1961. Ces instruments comprennent les Actes de l’OCDE (les Décisions et Recommandations adoptées par le Conseil de l’OCDE conformément à la Convention relative à l’OCDE) et d’autres instruments juridiques développés dans le cadre de l’OCDE (notamment les Déclarations et les accords internationaux).

L’ensemble des instruments juridiques de substance de l’OCDE, qu’ils soient en vigueur ou abrogés, est répertorié dans le Recueil des instruments juridiques de l’OCDE. Ils sont présentés selon cinq catégories :

- Les **Décisions** sont adoptées par le Conseil et sont juridiquement contraignantes pour tous les Membres, à l’exception de ceux qui se sont abstenus au moment de leur adoption. Elles définissent des droits et des obligations spécifiques et peuvent prévoir des mécanismes de suivi de la mise en œuvre**.**
- Les **Recommandations** sont adoptées par le Conseil et n’ont pas une portée juridique obligatoire. Elles représentent un engagement politique vis-à-vis des principes qu’elles contiennent, il est attendu que les Adhérents feront tout leur possible pour les mettre en œuvre.
- Les **Documents finaux de substance** sont adoptés individuellement par les Adhérents indiqués plutôt que par un organe de l’OCDE et sont le résultat d’une réunion ministérielle, à haut niveau ou autre, tenue dans le cadre de de l’Organisation. Ils énoncent habituellement des principes généraux ou des objectifs à long terme et ont un caractère solennel.
- Les **accords internationaux** sont négociés et conclus dans le cadre de l’Organisation. Ils sont juridiquement contraignants pour les parties.
- **Arrangement, accord/arrangement et autres** : plusieurs autres types d’instruments juridiques de substance ont été développés dans le cadre de l’OCDE au fil du temps, comme l’Arrangement sur les crédits à l’exportation bénéficiant d’un soutien public, l’Arrangement international sur les Principes à suivre dans les transports maritimes et les Recommandations du Comité d’aide au développement (CAD).