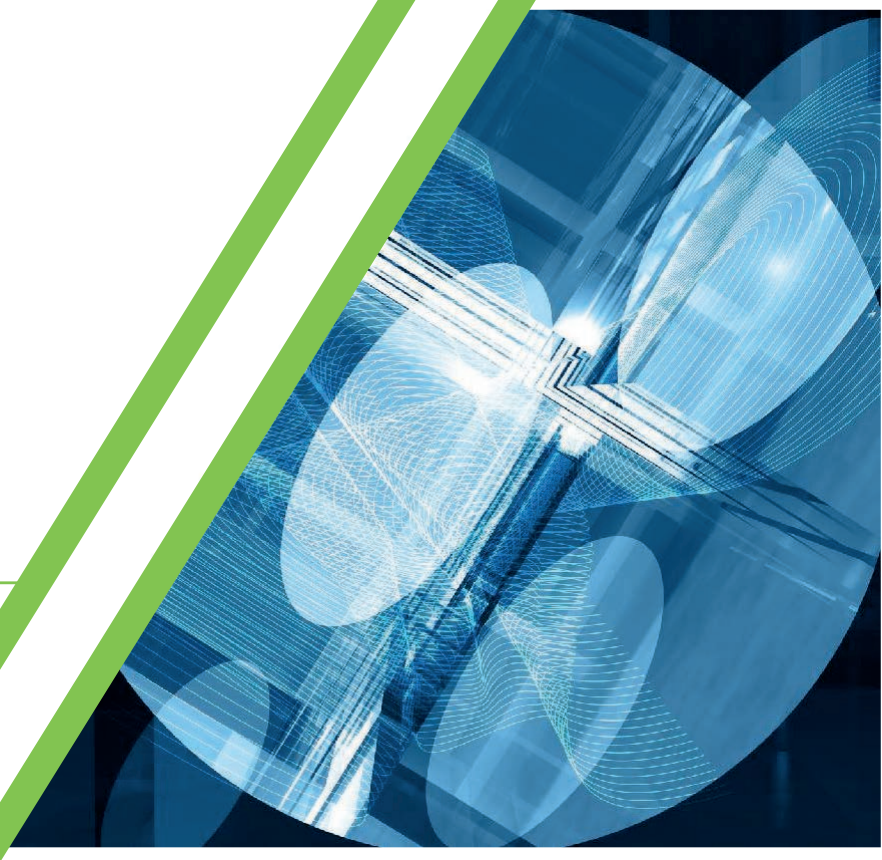
Recommandation du Conseil relative aux Lignes directrices régissant la politique de cryptographie



Instruments juridiques de l'OCDE

OCDE
DES POLITIQUES MEILLEURES POUR UNE VIE MEILLEURE

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

Date(s)

Adopté(e) le 27/03/1997

Informations Générales

La Recommandation relative aux Lignes directrices régissant la politique de cryptographie a été adoptée par le Conseil de l'OCDE le 27 mars 1997 sur proposition du Comité de la politique de l'information, de l'informatique et des communications (désormais appelé Comité de la politique de l'économie numérique). La Recommandation portent sur les questions à prendre en compte dans la formulation des politiques relatives à la cryptographie aux niveaux national et international : elle promeut l'utilisation de systèmes cryptographiques qui assurent l'interopérabilité, la portabilité et la mobilité, et sont d'un bon rapport coût-efficacité ; elle favorise la confiance dans les infrastructures et services numériques; contribue à assurer la sécurité des données ; et à protéger la vie privée sans mettre indûment en péril la sécurité publique, le respect des lois et la sécurité nationale.

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.

Adhérents*

Membres de l'OCDE	Non-Membres
Allemagne	Turquie
Australie	
Autriche	
Belgique	
Canada	
Chili	
Corée	
Danemark	
Espagne	
Estonie	
États-Unis	
Finlande	
France	
Grèce	
Hongrie	
Irlande	
Islande	
Israël	
Italie	
Japon	
Lettonie	
Lituanie	
Luxembourg	
Mexique	
Norvège	
Nouvelle-Zélande	
Pays-Bas	
Pologne	
Portugal	
République slovaque	
République tchèque	
Royaume-Uni	
Slovénie	
Suède	
Suisse	

*Des informations complémentaires ainsi que des déclarations sont disponibles sur le Recueil des instruments juridiques de l'OCDE : http://legalinstruments.oecd.org

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 Corée, 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 Turquie. L'Union européenne participe aux travaux de l'OCDE.

Instruments juridiques de l'OCDE

Environ 450 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 :

- **Décisions** : instruments juridiques de l'OCDE juridiquement contraignants pour tous les Membres, à l'exception de ceux qui se sont abstenus au moment de leur adoption. Bien qu'elles ne constituent pas des traités internationaux, elles impliquent le même type d'obligations juridiques. Les Adhérents ont l'obligation de mettre en œuvre les Décisions et doivent prendre les mesures nécessaires à cette mise en œuvre.
- **Recommandations** : instruments juridiques de l'OCDE n'ayant pas une portée juridique obligatoire, la pratique leur reconnaît cependant une force morale importante dans la mesure où elles représentent la volonté politique des Adhérents. Il est dès lors attendu que les Adhérents fassent tout ce qui est en leur pouvoir pour les mettre en œuvre intégralement. Par conséquent, lorsqu'un Membre n'a pas l'intention de mettre en œuvre une Recommandation, il s'abstient lors de son adoption, bien que cela ne soit pas requis juridiquement.
- **Déclarations** : instruments juridiques de l'OCDE préparés au sein de l'Organisation, généralement dans le cadre d'un organe subsidiaire. Elles énoncent habituellement des principes généraux ou des objectifs à long terme, ont un caractère solennel et sont adoptées à l'occasion de réunions ministérielles du Conseil ou de comités de l'Organisation.
- **Accords internationaux** : instruments juridiques de l'OCDE négociés et conclus dans le cadre de l'Organisation. Ils sont juridiquement contraignants pour les parties.
- **Arrangement, accord/arrangement et autres** : plusieurs instruments juridiques de substance ad hoc 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).