Recommandation du Conseil concernant les lignes directrices régissant la sécurité des systèmes d'information

Instruments juridiques de l'OCDE

OCDE
DES POLITIQUES MEILLEURES POUR UNE VIE MEILLEURE

Merci de citer cet ouvrage comme suit :
OCDE, *Recommandation du Conseil concernant les lignes directrices régissant la sécurité des systèmes d'information*, OECD/LEGAL/0271

Collection : Instruments juridiques de l'OCDE

Date(s)

Adopté(e) le 26/11/1992
Abrogé(e) le 25/07/2002

LE CONSEIL,

VU :

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

2. 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)] ;

3. 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] ;

RECONNAISSANT :

1. l'utilisation et la valeur croissantes des ordinateurs, installations de communication, réseaux d'ordinateurs et de communication, ainsi que des données et informations qu'ils permettent de conserver, de traiter, d'extraire ou de transmettre, y compris les programmes, spécifications et procédures destinés à leur fonctionnement, utilisation et maintenance (ci-après désignés collectivement par l'expression « systèmes d'information ») ;

2. le caractère international des systèmes d'information et leur expansion à l'échelle mondiale ;

3. le fait que, comme les systèmes d'information jouent un rôle de plus en plus grand dans les activités économiques et dans les échanges, sur le plan national et international, ainsi que dans la vie sociale, culturelle et politique, et que la dépendance à leur égard s'accroît, des efforts particuliers s'imposent afin de susciter la confiance dans les systèmes d'information ;

4. le fait qu'en l'absence de mesures de protection adaptées, les données et informations se trouvant sur des systèmes d'information acquièrent, par rapport aux supports papier, une sensibilité et une vulnérabilité particulières en raison des risques inhérents aux moyens d'accès, d'utilisation, d'appropriation abusive, d'altération et de destruction sans autorisation ;

5. la nécessité de sensibiliser aux risques menaçant les systèmes d'information et aux moyens de se prémunir contre ces risques ;

6. le fait que les mesures, pratiques, procédures et institutions actuelles ne répondent peut-être pas de façon appropriée aux nouveaux problèmes que posent les systèmes d'information, ni aux impératifs concomitants de clarté, de prévisibilité, de certitude et d'uniformité des droits et devoirs, de respect de ces droits, de moyens de recours et de réparation en cas de violation des droits relatifs aux systèmes d'information et à leur sécurité ;

7. l'avantage d'une plus grande coordination et coopération internationales en vue de répondre aux problèmes posés par les systèmes d'information, les éventuels effets préjudiciables d'un manque de coordination et de coopération sur les activités économiques et les échanges au plan tant national qu'international, ainsi que sur la participation à la vie sociale, culturelle et politique, de même que l'intérêt commun à promouvoir la sécurité des systèmes d'information ;

RECONNAISSANT EN OUTRE :

1. que les Lignes directrices n'affectent pas les droits souverains des Etats en ce qui concerne la sécurité nationale et l'ordre public, lesquels demeurent régis par la législation nationale ;

2. que, dans le cas particulier des pays à structure fédérale, la répartition des pouvoirs dans la Fédération peut avoir une incidence sur l'application des Lignes directrices ;

RECOMMANDE AUX PAYS MEMBRES :

1. d'établir des mesures, pratiques et procédures qui traduisent les principes relatifs à la sécurité des systèmes d'information énoncés dans les Lignes directrices figurant dans l'Appendice à la présente Recommandation qui en fait partie intégrante ;

2. de faire en sorte que la mise en œuvre des Lignes directrices s'accompagne de consultations, d'une coordination et d'une coopération, notamment d'une collaboration internationale en vue d'élaborer des normes, mesures, pratiques et procédures compatibles pour la sécurité des systèmes d'information ;

3. de convenir le plus rapidement possible d'initiatives spécifiques en vue de l'application des Lignes directrices ;

4. de donner une large diffusion aux principes énoncés dans les Lignes directrices ;

5. de réexaminer les Lignes directrices tous les cinq ans en vue d'améliorer la coopération internationale sur les questions concernant la sécurité des systèmes d'information.

APPENDICE

LIGNES DIRECTRICES RÉGISSANT LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

I. FINALITÉS

Les présentes Lignes directrices visent à :

a) sensibiliser aux risques menaçant les systèmes d'information et aux moyens disponibles pour se prémunir contre ces risques ;

b) créer un cadre général pour aider les personnes chargées, dans les secteurs public et privé, d'élaborer et de mettre en œuvre des mesures, des pratiques et des procédures cohérentes en vue d'assurer la sécurité des systèmes d'information ;

c) promouvoir la coopération entre les secteurs public et privé pour l'élaboration et la mise en œuvre de telles mesures, pratiques et procédures ;

d) susciter la confiance dans les systèmes d'information ainsi que dans leurs modes de fourniture et d'utilisation ;

e) faciliter la mise au point et l'utilisation de systèmes d'information au plan national et international ;

f) promouvoir la coopération internationale en vue d'assurer la sécurité des systèmes d'information.

II. CHAMP D'APPLICATION

Les Lignes directrices s'adressent aux secteurs public et privé.

Les Lignes directrices s'appliquent à tous les systèmes d'information.

Les Lignes directrices sont susceptibles d'être complétées par des mesures, pratiques et procédures additionnelles visant à assurer la sécurité des systèmes d'information.

III. DÉFINITIONS

Aux fins des présentes Lignes directrices :

a) par « données », on entend une représentation de faits, de concepts ou d'instructions sous une forme adaptée à la communication, à l'interprétation ou au traitement par des êtres humains ou des machines ;

b) par « informations », on entend la signification que prennent les données du fait des conventions qui s'attachent à ces données ;

c) par « systèmes d'information », on entend les ordinateurs, installations de communication et réseaux d'ordinateurs et de communication ainsi que les données et informations qu'ils permettent de conserver, de traiter, d'extraire ou de transmettre, y compris les programmes, spécifications et procédures destinés à leur fonctionnement, utilisation et maintenance ;

d) par « disponibilité », on entend, pour des données, informations ou systèmes d'information, le fait d'être accessibles et utilisables en temps voulu et de la manière requise ;

e) par « confidentialité », on entend, pour des données ou informations, le fait d'être uniquement portées à la connaissance des personnes, entités ou mécanismes autorisés, à des moments autorisés et d'une manière autorisée ;

f) par « intégrité », on entend, pour des données ou informations, le fait d'être exactes et complètes et la préservation de ce caractère exact et complet.

IV. OBJECTIF DE SÉCURITÉ

La sécurité des systèmes d'information a pour objectif de protéger les intérêts de ceux qui comptent sur les systèmes d'information, contre les préjudices imputables à des défauts de disponibilité, de confidentialité et d'intégrité.

V. PRINCIPES

Principe de responsabilité

1. Les attributions et responsabilités des propriétaires, fournisseurs et utilisateurs de systèmes d'information et autres parties concernées par la sécurité des systèmes d'information devraient être explicites.

Principe de sensibilisation

2. En vue de susciter la confiance à l'égard des systèmes d'information, les propriétaires, fournisseurs et utilisateurs de systèmes d'information et autres parties devraient pouvoir facilement, de manière compatible avec le maintien de la sécurité, avoir une connaissance appropriée et être informés de l'existence et de l'ampleur générale des mesures, pratiques et procédures visant à la sécurité des systèmes d'information.

Principe d'éthique

3. Les systèmes d'information devraient être fournis et utilisés, et leur sécurité devrait être mise œuvre de façon à ce que les droits et les intérêts légitimes des tiers soient respectés.

Principe de pluridisciplinarité

4. Les mesures, pratiques et procédures visant à la sécurité des systèmes d'information devraient prendre en compte et aborder toutes les considérations et tous les points de vue y afférents, qu'ils soient notamment techniques, administratifs, qu'ils concernent l'organisation, l'exploitation, le commerce, l'éducation ou le droit.

Principe de proportionnalité

5. Les niveaux, coûts, mesures, pratiques et procédures de sécurité devraient être appropriés et proportionnés à la valeur et au degré de dépendance à l'égard des systèmes d'information, ainsi qu'à la gravité, à la probabilité et à l'ampleur des éventuels préjudices, étant donné que les besoins en matière de sécurité varient selon les systèmes d'information.

Principe d'intégration

6. Les mesures, pratiques et procédures visant à la sécurité des systèmes d'information devraient être coordonnées et harmonisées entre elles et avec les autres mesures, pratiques et procédures de l'organisation de façon à créer un dispositif de sécurité cohérent.

Principe d'opportunité

7. Les intervenants publics et privés, au plan tant national qu'international, devraient agir en temps opportun, de manière coordonnée, afin d'empêcher les atteintes à la sécurité des systèmes d'information et d'y faire face.

Principe de réévaluation

8. La sécurité des systèmes d'information devrait être réévaluée périodiquement, étant donné que les systèmes d'information et les exigences en matière de sécurité varient dans le temps.

Principe de démocratie

9. La sécurité des systèmes d'information devrait être compatible avec l'utilisation et la circulation légitimes des données et informations dans une société démocratique.

VI. MISE EN OEUVRE

Les gouvernements, le secteur public et le secteur privé devraient prendre des mesures afin de protéger les systèmes d'information et d'assurer leur sécurité conformément aux Principes énoncés dans les Lignes directrices. Pour la réalisation de l'Objectif de sécurité et la mise en œuvre des Principes énoncés dans ces Lignes directrices, ils sont instamment invités, le cas échéant, à établir des mesures, pratiques, procédures et institutions de nature juridique, administrative, d'autodiscipline ou autre, afin d'assurer la sécurité des systèmes d'information et à encourager et soutenir l'établissement de telles dispositions. Lorsqu'ils n'ont pas encore pris de dispositions, ils devraient en particulier :

Élaboration de politiques

a) Adopter et encourager l'adoption de politiques, lois, décrets, règles et accords internationaux, en prévoyant notamment :

l'harmonisation des normes techniques, méthodes et codes de pratique à l'échelle mondiale ;

le développement de compétences techniques et de règles de l'art meilleures en matière de sécurité des systèmes d'information ;

l'établissement et la validité des contrats et autres documents créés et exécutés dans le cadre ou au moyen de systèmes d'information ;

la répartition des risques et de la responsabilité en cas de défaillances de la sécurité des systèmes d'information ;

des sanctions pénales, administratives ou autres en cas d'utilisation abusive des systèmes d'information ;

la compétence juridictionnelle des tribunaux, y compris des règles sur une compétence extraterritoriale, ainsi que la compétence administrative des autres organes ;

l'assistance mutuelle, l'extradition et d'autres formes de coopération internationale dans les affaires ayant trait à la sécurité des systèmes d'information ; et

les modalités d'obtention de preuves dans les systèmes d'information ainsi que la recevabilité de ces preuves dans le cadre de procédures civiles, pénales ou administratives.

Éducation et formation

b) Favoriser une sensibilisation aux impératifs et objectifs de la sécurité des systèmes d'information, notamment :

une conduite morale dans l'utilisation des systèmes d'information ; et

l'adoption de bonnes pratiques en matière de sécurité.

c) Assurer et encourager l'éducation et la formation :

des concepteurs, propriétaires, fournisseurs et utilisateurs des systèmes d'information ;

des spécialistes et auditeurs des systèmes d'information ;

des spécialistes et auditeurs de la sécurité des systèmes d'information ; et

des autorités chargées de l'application de la loi, enquêteurs, procureurs, avocats et juges.

Respect des droits et réparation

d) Donner de manière accessible et adéquate des moyens d'exercer et de faire respecter les droits résultant de la mise en œuvre des Lignes directrices et des moyens de recours et de réparation des violations de ces droits.

e) Offrir rapidement assistance dans les procédures et enquêtes concernant les atteintes à la sécurité des systèmes d'information.

Échanges d'informations

f) Faciliter les échanges d'informations concernant les Lignes directrices et leur mise en œuvre.

g) Assurer une bonne publicité des mesures, pratiques et procédures adoptées conformément aux Lignes directrices et concernant la sécurité des systèmes d'information.

Coopération

h) Sur le plan national et international, mener avec les autres gouvernements et avec le secteur privé des actions de consultation, coordination et coopération, afin d'encourager la mise en œuvre des Lignes directrices et d'harmoniser aussi complètement que possible les mesures, pratiques et procédures visant à la sécurité des systèmes d'information.

Adhérents*

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

*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, 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).