Recommandation du Conseil sur la gestion du risque de sécurité numérique pour la prospérité économique et sociale

17 septembre 2015 – C(2015)115

LE CONSEIL,

CONSIDÉRANT la Convention relative à l'Organisation de coopération et de développement économiques en date du 14 décembre 1960, notamment ses articles 1 b), 1 c), 3 a), 3 b) et 5 b) ;

CONSIDÉRANT la Recommandation du Conseil concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel (« Lignes directrices de l'OCDE sur la vie privée ») [C(80)58/FINAL, telle qu'amendée] ; la Recommandation du Conseil relative aux Lignes directrices régissant la politique de cryptographie [C(97)62/FINAL] ; la Recommandation du Conseil sur la protection des infrastructures d'information critiques [C(2008)35] ; la Déclaration sur le futur de l'économie Internet (la Déclaration de Séoul) [C(2008)99] ; la Recommandation du Conseil sur les principes pour l'élaboration des politiques de l'Internet [C(2011)154] ; la Recommandation du Conseil concernant la politique et la gouvernance réglementaires [C(2012)37] ; la Recommandation du Conseil sur les stratégies numériques gouvernementales [C(2014)88] ; et la Recommandation du Conseil sur la gouvernance des risques majeurs [C/MIN(2014)8/FINAL] ;

CONSIDÉRANT la Recommandation du Conseil concernant les Lignes directrices régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité [C(2002)131/FINAL], que la présente Recommandation remplace ;

RECONNAISSANT que l'environnement numérique, notamment l'Internet, est essentiel au fonctionnement de nos économies et de nos sociétés et qu'il stimule la croissance, l'innovation, le bien-être et l'inclusivité ;

RECONNAISSANT que les bienfaits qu'apporte l'environnement numérique, qui s'étendent à tous les secteurs de l'économie et à tous les aspects du progrès social, tiennent à la nature mondiale, ouverte, interconnectée et dynamique des technologies et de l'infrastructure de l'information et des communications, en particulier de l'Internet ;

RECONNAISSANT que l'utilisation, la gestion et le développement de l'environnement numérique sont soumis à des incertitudes qui sont dynamiques par nature ;

RECONNAISSANT que la gestion du risque de sécurité numérique relève d'une approche souple et réactive destinée à traiter ces incertitudes et tirer pleinement parti des bienfaits économiques et sociaux attendus, fournir les services essentiels et exploiter les infrastructures critiques, préserver les droits de l'homme et les valeurs fondamentales, et protéger les individus contre les menaces de sécurité numérique ;

SOULIGNANT que la gestion du risque de sécurité numérique fournit une base solide pour la mise en œuvre du « Principe des garanties de sécurité » énoncé dans les Lignes directrices de l'OCDE sur la vie privée et, plus généralement, que la présente Recommandation et lesdites Lignes directrices se renforcent mutuellement ;

CONSCIENT que les gouvernements, les organisations publiques et privées, ainsi que les individus partagent la responsabilité, selon leurs rôles respectifs et le contexte, de la gestion du risque de sécurité et de la protection de l'environnement numérique ; et que la coopération est essentielle aux niveaux national, régional et international.

Sur proposition du Comité de la politique de l'économie numérique :

I. RECOMMANDE que les Membres et les non-Membres qui adhèrent à la présente Recommandation (ci-après les « Adhérents ») :

1. Mettent en pratique les principes énoncés dans la section 1 (ci-après les « Principes ») à tous les niveaux du gouvernement et au sein des organisations publiques ;

2. Adoptent une stratégie nationale pour la gestion du risque de sécurité numérique telle que décrite dans la section 2 ;

II. APPELLE les décideurs au plus haut niveau du gouvernement et des organisations publiques et privées à adopter une approche de la gestion du risque de sécurité numérique pour susciter la confiance et tirer parti de l'environnement numérique ouvert afin d'assurer la prospérité économique et sociale ;

III. ENCOURAGE les organisations privées à intégrer les Principes à leur approche de la gestion du risque de sécurité numérique ;

IV. ENCOURAGE l'ensemble des parties prenantes à mettre en œuvre les Principes dans le cadre de leurs processus décisionnels, selon leurs rôles, leur capacité à agir et le contexte ;

V. APPELLE les gouvernements et les organisations publiques et privées à travailler de concert pour permettre aux individus et aux petites et moyennes entreprises de gérer de manière collaborative le risque de sécurité numérique ;

VI. CONVIENT que les Principes sont complémentaires et doivent être pris comme un tout, et qu'ils ont vocation à être en adéquation avec les processus, les bonnes pratiques, les méthodologies et les normes en matière de gestion du risque ;

VII. CONVIENT en outre qu'aux fins de la présente Recommandation :

1. Le risque est l'effet de l'incertitude sur l'atteinte des objectifs. Le terme « risque de sécurité numérique » désigne une catégorie de risque liée à l'utilisation, au développement et à la gestion de l'environnement numérique dans le cadre d'une activité quelle qu'elle soit. Ce risque peut résulter d'une combinaison de menaces et de vulnérabilités inhérentes à l'environnement numérique. Il peut compromettre la réalisation des objectifs économiques et sociaux en portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des activités et/ou de l'environnement. Dynamique par nature, le risque de sécurité numérique se compose d'éléments liés à l'environnement numérique, à l'environnement physique, aux personnes impliquées dans l'activité et aux processus organisationnels qui la structurent.
2. La « gestion du risque de sécurité numérique » est l'ensemble des mesures coordonnées, intra et/ou interorganisations, prises pour maîtriser le risque de sécurité numérique tout en maximisant les opportunités. Elle fait partie intégrante du processus décisionnel et s'inscrit dans un cadre global de gestion du risque qui pèse sur les activités économiques et sociales. Elle s'appuie sur un ensemble holistique, systématique et flexible de processus cycliques, aussi transparent et explicite que possible. Cet ensemble de processus contribue à la mise en œuvre de mesures de gestion du risque de sécurité numérique (« mesures de sécurité ») adaptées et proportionnées au risque et aux objectifs économiques et sociaux en jeu.

3. Les « parties prenantes » sont les gouvernements, les organisations publiques et privées et les individus qui dépendent de l'environnement numérique pour tout ou partie de leurs activités économiques et sociales. Elles peuvent endosser plusieurs rôles. « Les dirigeants et les décideurs » sont les acteurs opérant au plus haut niveau au sein du gouvernement et des organisations publiques et privées.

SECTION 1. PRINCIPES

Principes généraux

1. *Sensibilisation, compétences et autonomisation*

Toutes les parties prenantes devraient comprendre le risque de sécurité numérique et les moyens de le gérer.

Elles devraient être conscientes que le risque de sécurité numérique peut compromettre la réalisation de leurs objectifs économiques et sociaux, et que la gestion de ce risque peut avoir des incidences sur autrui. Elles devraient bénéficier de l'éducation et des compétences nécessaires pour comprendre ce risque, pour aider à le maîtriser et pour évaluer l'impact que pourraient avoir leurs décisions en matière de gestion du risque de sécurité numérique, tant sur leurs activités que sur l'ensemble de l'environnement numérique.

2. *Responsabilité*

Toutes les parties prenantes devraient assumer la responsabilité de la gestion du risque de sécurité numérique.

Elles devraient faire preuve de responsabilité et être en mesure de répondre, selon leurs rôles, le contexte et leur capacité à agir, de la gestion du risque de sécurité numérique et de la prise en compte de l'impact potentiel de leurs décisions sur autrui. Elles devraient par ailleurs reconnaître qu'un certain niveau de risque de sécurité numérique doit être accepté pour atteindre les objectifs économiques et sociaux.

3. *Droits de l'homme et valeurs fondamentales*

Toutes les parties prenantes devraient gérer le risque de sécurité numérique de manière transparente, dans le respect des droits de l'homme et des valeurs fondamentales.

La gestion du risque de sécurité numérique devrait se faire dans le respect des droits de l'homme et des valeurs fondamentales reconnues par les sociétés

démocratiques, notamment la liberté d'expression, la libre circulation de l'information, la confidentialité de l'information et des communications, la protection de la vie privée et des données à caractère personnel, l'ouverture et le droit à une procédure équitable. La gestion du risque de sécurité numérique devrait se fonder sur un comportement éthique qui respecte et reconnaisse les intérêts légitimes d'autrui et de la société dans son ensemble. Les organisations devraient se doter d'une politique générale de transparence quant à leurs pratiques et leurs procédures de gestion du risque de sécurité numérique.

4. *Coopération*

Toutes les parties prenantes devraient coopérer, y compris au-delà des frontières.

Le caractère mondialement interconnecté de l'environnement numérique se traduit par une interdépendance des parties prenantes et nécessite une coopération en matière de gestion du risque de sécurité. Cette coopération, qui est l'affaire de tous, doit se faire non seulement au sein des gouvernements et des organisations publiques et privées, mais aussi entre elles/eux, ainsi qu'avec les individus. En outre, elle devrait s'étendre au-delà des frontières, aux niveaux régional et international.

Principes opérationnels

5. *Cycle d'évaluation et de traitement du risque*

Les dirigeants et les décideurs devraient s'assurer que le traitement du risque de sécurité numérique est fondé sur une évaluation permanente du risque.

L'évaluation du risque de sécurité numérique devrait s'inscrire dans un processus systématique et cyclique permanent. Elle devrait estimer les conséquences que les menaces, conjuguées aux vulnérabilités, pourraient avoir sur les activités économiques et sociales en jeu, et éclairer le processus décisionnel afférent au traitement du risque. Ledit traitement devrait viser à réduire le risque à un niveau acceptable au regard des bienfaits économiques et sociaux que l'on attend de ces activités, tout en tenant compte des incidences potentielles sur les intérêts légitimes d'autrui. Le traitement du risque peut prendre plusieurs formes : accepter le risque, le réduire, le transférer, l'éviter, ou opter pour une combinaison de ces approches.

6. *Mesures de sécurité*

Les dirigeants et les décideurs devraient s'assurer que les mesures de sécurité sont appropriées et proportionnées au risque.

L'évaluation du risque de sécurité numérique devrait guider le choix, la mise en œuvre et l'amélioration des mesures de sécurité prises pour réduire le risque au niveau acceptable tel que défini lors de l'évaluation et du traitement de ce risque. Ces mesures devraient être appropriées et proportionnées au risque, et choisies en tenant compte des effets négatifs et positifs qu'elles pourraient avoir sur les activités économiques et sociales qu'elles visent à protéger, ainsi que sur les droits de l'homme et les valeurs fondamentales, et sur les intérêts légitimes d'autrui. Tous les types de mesures devraient être envisagés, que ces mesures soient physiques ou numériques, ou qu'elles s'appliquent aux personnes, aux processus ou aux technologies concernés par les activités. Les organisations devraient rechercher les vulnérabilités et y apporter une réponse appropriée dans les plus brefs délais.

7. *Innovation*

Les dirigeants et les décideurs devraient s'assurer que l'innovation est prise en considération.

L'innovation devrait faire partie intégrante de la réduction du risque de sécurité numérique au niveau acceptable fixé lors de l'évaluation et du traitement de ce risque. Elle devrait jouer un rôle à la fois dans la conception et la conduite des activités économiques et sociales qui dépendent de l'environnement numérique, et dans l'élaboration et la mise en place des mesures de sécurité.

8. *Préparation et continuité*

Les dirigeants et les décideurs devraient s'assurer de l'adoption d'un plan de préparation et de continuité.

À partir de l'évaluation du risque de sécurité numérique, un plan de préparation et de continuité devrait être adopté pour atténuer les effets préjudiciables des incidents de sécurité et favoriser la continuité et la résilience des activités économiques et sociales. Il devrait recenser les mesures permettant de prévenir les incidents de sécurité numérique, de les détecter, d'y répondre et d'assurer la reprise des activités. Il devrait en outre prévoir des mécanismes attribuant des niveaux d'escalade clairs en fonction de l'ampleur et de la gravité des effets

de ces incidents, ainsi que de leur potentiel de propagation aux autres acteurs de l'environnement numérique. Des procédures de notification appropriées devraient être envisagées dans le cadre de la mise en œuvre du plan.

SECTION 2. STRATÉGIES NATIONALES

A. Les stratégies nationales de gestion du risque de sécurité numérique devraient être cohérentes avec les Principes et créer les conditions nécessaires à la gestion, par l'ensemble des parties prenantes, du risque de sécurité numérique qui pèse sur les activités économiques et sociales, et à l'instauration d'un climat de confiance dans l'environnement numérique. Pour ce faire, elles devraient :

1. Bénéficier du soutien des plus hautes instances du gouvernement et définir une approche claire et intergouvernementale qui soit souple, neutre sur le plan technologique et cohérente avec les autres stratégies en faveur de la prospérité économique et sociale ;

2. Énoncer clairement qu'elles visent à : tirer parti de l'environnement numérique ouvert pour favoriser la prospérité économique et sociale, en réduisant le niveau général de risque de sécurité numérique à l'échelle nationale et internationale, sans imposer de restrictions superflues à la circulation des technologies, des communications et des données ; et garantir la fourniture des services essentiels et le fonctionnement des infrastructures critiques, protéger les individus contre les menaces de sécurité numérique sans perdre de vue la nécessité de préserver la sécurité nationale et internationale, et protéger les droits de l'homme et les valeurs fondamentales ;

3. S'adresser à toutes les parties prenantes, être adaptées, s'il y a lieu, aux petites et moyennes entreprises et aux individus, et énoncer la responsabilité des parties prenantes et leur obligation de rendre des comptes, selon leurs rôles, leur capacité à agir et le contexte dans lequel elles opèrent ;

4. Être le fruit d'une approche intragouvernementale coordonnée et d'un processus de consultation ouvert et transparent associant toutes les parties prenantes, être régulièrement révisées et améliorées à la lumière des expériences et des bonnes pratiques en utilisant, si possible, des mesures comparables à l'échelle internationale.

B. Les stratégies nationales devraient comprendre des mesures aux termes desquelles les gouvernements :

*1. **Donnent l'exemple,** et notamment :*

i) Adoptent un cadre complet pour gérer le risque de sécurité numérique qui pèse sur leurs propres activités. Ce cadre et les politiques de mise en œuvre devraient être transparents afin de susciter la confiance dans les activités et le comportement du gouvernement, y compris pour ce qui est de la divulgation responsable des vulnérabilités qu'ils ont détectées et des mesures d'atténuation des risques prises en conséquence ;

ii) Mettent en place des mécanismes de coordination associant tous les acteurs concernés au sein du gouvernement, afin de s'assurer que leur gestion du risque de sécurité numérique est compatible et concourt à faire progresser la prospérité économique et sociale ;

iii) S'assurent de la création, au niveau national, d'au moins une équipe de réponse aux incidents de sécurité informatique (CSIRT), également appelée équipe d'intervention en cas d'urgence informatique (CERT) et, s'il y a lieu, encourager l'émergence de CSIRT publiques et privées travaillant en collaboration, y compris avec celles d'autres pays ;

iv) Utilisent leur position sur le marché pour promouvoir la gestion du risque de sécurité numérique dans l'ensemble de l'économie et de la société, notamment au travers des politiques de passation de marchés publics et du recrutement de spécialistes possédant les qualifications nécessaires en matière de gestion du risque ;

v) Encouragent l'utilisation de normes et de bonnes pratiques internationales de gestion du risque de sécurité numérique et en favorisent le développement et l'examen par le biais de processus ouverts, transparents et multi-partites ;

vi) Adoptent des techniques de sécurité innovantes pour gérer le risque de sécurité numérique, afin de garantir une protection adéquate des informations stockées et en transit, en tenant compte de l'intérêt d'imposer des restrictions appropriées à la collecte et la conservation des données ;

vii) Coordonnent et promeuvent la recherche et le développement publics en matière de gestion du risque de sécurité numérique afin de stimuler l'innovation ;

viii) Favorisent le développement d'une main-d'œuvre qualifiée capable de gérer le risque de sécurité numérique, en particulier en intégrant cette discipline dans les stratégies globales sur les compétences. Pour ce faire, les pouvoirs publics pourraient miser sur la formation continue et la certification dans le domaine de la gestion du risque, et soutenir le développement des compétences numériques au sein de la population, par le biais des programmes nationaux d'éducation, notamment dans l'enseignement supérieur ;

ix) Adoptent et mettent en œuvre un cadre global de lutte contre la cybercriminalité, en s'appuyant sur les instruments internationaux existants ;

x) Allouent des ressources suffisantes pour une mise en œuvre efficace des stratégies.

2. Renforcent la coopération internationale et l'assistance mutuelle, *et notamment :*

i) Prennent part à des forums régionaux et internationaux dans le domaine, et nouent des relations bilatérales et multilatérales pour favoriser le partage d'expériences et de bonnes pratiques ; et promeuvent une approche de la gestion du risque de sécurité numérique à l'échelle nationale qui ne fasse pas peser un risque accru sur les autres pays ;

ii) Dispensent, à titre volontaire, assistance et soutien à d'autres pays qui en auraient besoin et établissent des points de contact nationaux pour que les demandes de pays étrangers liées aux questions de gestion du risque de sécurité numérique puissent être traitées en temps utile ;

iii) S'efforcent d'améliorer la réponse aux menaces d'origine nationale ou étrangère, par le biais, notamment, de la coopération entre les CSIRT, d'exercices coordonnés et d'autres instruments de collaboration.

3. Collaborent avec d'autres parties prenantes, *et notamment :*

i) Réfléchissent à la manière dont les gouvernements et les autres parties prenantes peuvent s'entraider afin de mieux gérer le risque de sécurité numérique pesant sur leurs activités ;

ii) Recensent et atténuent de possibles effets négatifs que les politiques menées par les pouvoirs publics pourraient avoir sur les activités des autres parties prenantes ou sur la prospérité économique et sociale du pays ;

iii) Établissent des pratiques et des procédures de gestion du risque de sécurité numérique et les font connaître publiquement ;

iv) Encouragent la détection, le signalement et/ou la correction des vulnérabilités de sécurité numérique par toutes les parties prenantes, dans un esprit de responsabilité ;

v) Renforcent la sensibilisation, les compétences et l'autonomisation à l'échelle de la société, afin de favoriser la gestion du risque de sécurité numérique au moyen d'initiatives neutres du point de vue technologique et adaptées aux besoins particuliers des différentes catégories de parties prenantes.

4. ***Créent les conditions propices à une collaboration de toutes les parties prenantes à la gestion du risque de sécurité numérique,*** *et notamment :*

i) Favorisent la participation active des parties prenantes concernées, dans un climat de confiance mutuelle, à des initiatives et des partenariats, qu'ils soient privés ou public-privé, formels ou informels, de niveau national, régional ou international, afin :
   - De partager des connaissances, des compétences, des expériences réussies et des pratiques éprouvées en matière de gestion du risque de sécurité numérique tant au niveau des politiques qu'au niveau opérationnel ;
   - D'échanger des informations concernant la gestion du risque de sécurité numérique ;
   - D'anticiper les enjeux et les opportunités à venir et de s'y préparer.

ii) Renforcent la coordination entre les parties prenantes afin d'améliorer, d'une part, la détection des vulnérabilités et des menaces et les mesures prises pour y remédier et, d'autre part, l'atténuation du risque de sécurité numérique ;

iii) Incitent l'ensemble des parties prenantes à travailler de concert pour aider à protéger les individus et les petites et moyennes entreprises contre les menaces, et renforcer leur capacité à gérer le risque de sécurité numérique qui pèse sur leurs activités économiques et sociales ;

iv) Créent, s'il y a lieu, des dispositifs pour inciter les parties prenantes à gérer le risque de sécurité numérique, et améliorer la transparence et l'efficience du marché ;

v) Encouragent l'innovation en matière de gestion du risque de sécurité numérique et de développement d'outils utilisables par les individus et les organisations pour protéger leurs activités dans l'environnement numérique ;

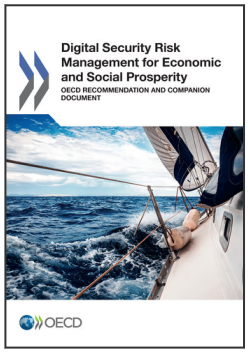
vi) Encouragent le développement d'indicateurs du risque permettant les comparaisons internationales, fondés sur des méthodologies, des normes et des bonnes pratiques communes, le cas échéant, afin d'améliorer l'efficacité, l'efficience et la transparence de la gestion du risque de sécurité numérique.

VIII. RECOMMANDE que les Adhérents travaillent de concert à la mise en œuvre de la présente Recommandation et en assurent la promotion et la diffusion dans les secteurs public et privé, auprès des non-Adhérents et dans les forums internationaux ;

IX. INVITE les non-Membres à adhérer à la présente Recommandation ;

X. CHARGE le Comité de la politique de l'économie numérique d'examiner la mise en œuvre de la présente Recommandation et d'en faire rapport au Conseil dans les trois ans suivant son adoption, puis ultérieurement en fonction des besoins.

***



Extrait de :

Digital Security Risk Management for Economic and Social Prosperity

OECD Recommendation and Companion Document

Accéder à cette publication :
https://doi.org/10.1787/9789264245471-en

Merci de citer ce chapitre comme suit :

OCDE (2015), « Recommandation du Conseil sur la gestion du risque de sécurité numérique pour la prospérité économique et sociale », dans *Digital Security Risk Management for Economic and Social Prosperity : OECD Recommendation and Companion Document*, Éditions OCDE, Paris.

DOI: https://doi.org/10.1787/9789264246089-1-fr

OCDE