Petit déjeuner débat du **4 novembre 2015**

LA NOUVELLE RECOMMANDATION DE L'OCDE

avec

M. Laurent BERNAT

Administrateur à la Division des Politiques de l'Economie Numérique, OCDE

sous la présidence de

Bénédicte PILLIET

Directeur du CyberCercle

COMPTE RENDU

La nouvelle Recommandation de l'OCDE sur la « *Gestion du Risque de Sécurité Numérique pour la Prospérité Économique et Sociale* » propose des principes novateurs, plus poussés qu'au préalable. Elle affirme que la cybersécurité ne doit pas freiner le développement économique et social mais qu'au contraire, elle doit le favoriser.

L'OCDE est une organisation intergouvernementale basée à Paris, et ses 34 pays membres sont considérés comme étant les « plus avancés ». Elle se distingue d'autres organisations par le fait qu'elle traite des questions touchant l'économie et la société sous l'angle des politiques publiques. L'OCDE n'aborde donc pas, sauf exception, les questions de sécurité et défense nationale, de renseignement ou de criminalité. Néanmoins, la proximité de ces questions avec certaines questions abordées par l'OCDE impose parfois l'implication de l'organisation dans ces sujets.
L'OCDE se concentre sur les politiques publiques et ne dispose pas de moyens opérationnels ou techniques, ce positionnement étant illustré par son slogan « *des politiques meilleures pour des vies meilleures* ».

L'OCDE touche aujourd'hui toutes les questions qui sont du ressort des gouvernements, sauf la sécurité et la défense en tant que telles. Sa spécificité d'analyse sous l'angle des politiques publiques fait que les Etats membres ont conscience de son intérêt. L'OCDE produit des Recommandations et des analyses qui ont une longueur d'avance par rapport aux analyses plus opérationnelles produites par d'autres organisations internationales.

Les pays membres apprécient l'OCDE, d'une part, pour son rôle de forum où ils peuvent partager leur expérience et dialoguer afin de progresser ensemble dans la même direction, ainsi que, d'autre part, pour sa production d'analyses et de Recommandations indépendantes qui sont en avance par rapport aux travaux d'autres acteurs.

Une Recommandation de l'OCDE est un instrument juridique non-contraignant, adopté par consensus. Les pays membres s'engagent à faire le nécessaire pour la mettre en œuvre.

La nouvelle Recommandation sur la « *Gestion du Risque de Sécurité Numérique pour la Prospérité Économique et Sociale* », si elle traite de cybersécurité, ne contient ce terme ni dans son titre, ni ailleurs. Durant le processus de rédaction, une certaine réticence à utiliser le préfixe « cyber » a rapidement émergé car il donnait le sentiment de constituer un champ à part, nécessitant une approche spécifique, ce qui était à l'opposé de la volonté de faire du risque numérique un type de risque comme un autre.

L'OCDE travaille sur la « cybersécurité » depuis plus plus de 20 ans, bien que sous d'autres vocables. Selon l'OCDE, il y a différents aspects à prendre en compte lorsque l'on traite de cybersécurité :

- L'aspect technique ;
- L'aspect de la lutte contre la criminalité ;
- L'aspect de sécurité nationale et internationale, qui a progressivement émergée dans le champ des politiques publiques de manière explicite depuis 2009.

A ces trois dimensions, s'ajoute celle de la prospérité économique et sociale, présente depuis l'émergence du numérique dans la société, notamment au travers des enjeux de confiance dans le numérique. C'est précisément cet aspect qu'approfondit la Recommandation de l'OCDE.

C'est l'évolution du contexte qui a justifiée l'élaboration de cette Recommandation qui remplace les Lignes directrices de l'OCDE sur la sécurité de 2002, elles-mêmes issues d'une Recommandation de 1992. Alors qu'en 1992 l'informatique était utile dans l'économie, en 2002 elle est devenue importante et aujourd'hui, elle est essentielle à tous les acteurs et dans tous les secteurs, à la fois pour le fonctionnement et le développement de l'économie. Le numérique est ainsi devenu un impératif pour

toutes les étapes de la chaine de la valeur, bien qu'on ait souvent tendance à l'assimiler uniquement à l'utilisateur final : le consommateur. On en oublie alors qu'aucun des autres maillons de la chaine de la valeur ne pourrait fonctionner et ni être amélioré sans bénéficier de l'innovation issue du numérique, répercutant ses bénéfices à l'entreprises, en termes d'innovations, de compétitivité et de croissance. Le numérique est également un facteur de progrès social, par exemple en matière d'éducation, d'amélioration des services de santé, ou encore de participation démocratique.

L'interconnectivité est plus que jamais présente dans notre société. Elle va encore s'accroître dans la mesure où, aujourd'hui, elle dépasse largement le strict secteur de l'informatique pour s'intégrer aux objets de tous les jours, le fameux *Internet of Things*. Cette tendance forte apporte d'importants bénéfices économiques et sociaux, ouvrant néanmoins la voie à de potentiel incidents de sécurité.

Les attaques portant atteinte à la sécurité du numérique se sont complexifiées et deviennent de plus en plus médiatisées. Elles touchent aujourd'hui tous les secteurs, et entraînent des fuites de données à grande échelle. Les entreprises et les gouvernements sont touchés par cette menace (exemple du hack de l'OPM aux Etats-Unis) qui comporte désormais un volet « physique ». Par exemple, l'autorité allemande en charge de la cybersécurité a diffusé un rapport faisant état de dégâts massifs dans une aciérie suite à une attaque cyber. Stuxnet n'est donc désormais plus la seule illustration de cyberattaque engendrant des dégâts physiques massifs.
Ces derniers mois ont également été marqués par un phénomène nouveau : les effets que des cyberattaques ont eus sur les équipes dirigeantes. De nombreux dirigeants d'entreprises ou de services gouvernementaux ont ainsi démissionné suite à des incidents de cybersécurité (ex-patronne de l'OPM, ancien co-dirigeant de Sony Pictures, PDG de Target Store, ou encore de grandes banques coréennes). Ces événements montrent que si les attaques semblent être de nature technique ou technologique, leurs conséquences dépassent la dimension technique et impactent également la société et l'économie. Cette situation défie notre conception traditionnelle « cybersécurité ». Il en ressort le double message de la nouvelle Recommandation :

1) L'approche classique de la sécurité ne fonctionne pas.

L'approche classique consistait à mettre en œuvre un périmètre autour de ce que l'on voulait protéger, pour faire en sorte que la menace ne le touche pas. Le terme « sécurité » renvoie d'ailleurs à un état dans lequel il n'y a pas de danger. Or cette conception ne fonctionne pas dans un environnement tel que le numérique qui, par nature, est ouvert pour favoriser les échanges et l'innovation.
S'il faut certes protéger et donc fermer dans une certaine mesure l'environnement numérique, le fermer par défaut impliquerait de renoncer au potentiel économique et social offert par l'ouverture. Il faut donc trouver le juste équilibre entre ouverture et fermeture. Mais comment calibrer le degré de fermeture ? Comment s'assurer que les mesures de sécurité en place ne nuiront pas à l'utilisation de l'environnement numérique pour innover, gagner en productivité, réduire les coûts, bref, augmenter la compétitivité ?

Par ailleurs, l'approche classique est basée sur un objectif absolu : la sécurité, c'est-à-dire l'élimination du risque. Or cet objectif est inatteignable tant dans l'environnement numérique que partout ailleurs. Ce qui renvoie à la première question : quel niveau de sécurité est approprié ? Comment choisir les mesures de sécurité pour qu'elles servent pleinement les objectifs économiques plutôt qu'un objectif abstrait et inatteignable de sécurité absolue ?

2) La cybersécurité est le risque économique et social lié à l'environnement numérique.

Face à ce constat, l'OCDE considère qu'il est donc nécessaire d'accepter un certain niveau de risque résiduel. Si le risque ne peut pas être entièrement éliminé, et s'il est donc impossible de créer un

environnement 100% sûr et sécurisé, le risque de sécurité peut cependant être réduit à un niveau acceptable à la lumière des activités économiques en jeu et en tenant compte du contexte. C'est le but de la gestion de risque.

Il ne faut donc pas confondre les fins et les moyens. Ce que l'on appelle la « sécurité » n'est qu'un moyen d'augmenter les chances de succès des activités économiques et sociales qui utilisent le numérique pour se rapprocher de la prospérité économique et sociale. Elle ne doit pas être comprise comme une fin. C'est l'autre raison pour laquelle le terme « cybersécurité » n'est pas utilisé dans la Recommandation.

Malheureusement, beaucoup d'acteurs ne comprennent pas que les concepts liés à la gestion de risque car les termes sont trompeurs. Par exemple, qu'est-ce que le risque ? Il est très courant de constater une confusion entre le risque et les facteurs de risque que sont les menaces, les vulnérabilités et les incidents. Du point de vue de l'OCDE, qui s'inspire en cela des travaux de l'ISO (ISO 31000 et ISO Guide 73), le risque est la conséquence d'une situation (l'incident) résultant de menaces exploitant des vulnérabilités.

Il faut par ailleurs distinguer le risque économique et social, celui qui lequel se concentre l'CODE, et qui concerne les dirigeants et les décideurs économiques (c'est-à-dire « métier »), du risque technique, qui est principalement l'affaire des informaticiens. Seuls les décideurs en charge de la réalisation des objectifs économiques et sociaux sont à même de fixer le niveau acceptable de risque de sécurité numérique et d'assumer la responsabilité de conséquences négatives possibles du choix de mesures de sécurité sur les activités économiques qu'elles sont supposées protéger. Et pour ce faire, les décideurs doivent bénéficier du concours des experts techniques. Plus généralement, la gestion du risque de sécurité numérique devrait être pleinement intégrée au processus de prise de décision économique et soutenue par les experts techniques.

Si une entreprise ou une organisation approche ce risque sous l'angle technique, elle échouera car le problème n'est principalement d'ordre technique, il est avant tout d'ordre économique.

Les personnes responsables de la gestion de risque devraient donc être celles qui ont également la responsabilité de la réalisation des objectifs économiques, qui reposent sur l'environnement numérique. Cette Recommandation s'adresse donc aux dirigeants, aux comités d'administration, aux décideurs en charge de l'activité économique en leur disant, en quelque sorte, qu'ils ne peuvent pas être uniquement responsables pour les bénéfices de l'intégration du numérique dans leurs processus, produits et services. Ils doivent aussi, de la même façon, être responsables pour la gestion des risques économiques qui en découlent.

La nouvelle Recommandation de l'OCDE sur la gestion du risque numérique comporte huit grands principes, dont certains sont plus novateurs.

- Les principes généraux partent de la nécessité d'être conscient de l'existence des risques, étape sans laquelle rien n'est possible. Puis, il faut également être conscient de comment gérer les risques, ce qui relève de la question des compétences.
- Le principe de responsabilité : toutes les parties prenantes partagent la responsabilité de gérer le risque de sécurité numérique, en fonction de leur rôle, de leur capacité à agir et du contexte. Elles doivent reconnaître qu'un certain niveau de risque doit être accepté, ce qui implique que quelqu'un soit responsable pour fixer le niveau de risque acceptable et assumer les conséquences lorsqu'un incident surviendra.
- Le principe de coopération : il inclut la coopération métier, public-privé, internationale, intra-gouvernementale et intersectorielle.

Suivent quatre principes opérationnels. Le risque doit d'abord être évalué et traité de façon continue. Sur cette base, les mesures de sécurité doivent être mises en place et maintenues, un plan de préparation doit être réalisé car il est quasi-certain que des incidents se produiront et il faudra avoir défini à l'avance des responsabilités pour les gérer et les processus pour continuer de réduire le risque tout en assurant la continuité des opérations (résilience). Enfin, le principe d'innovation : pour réduire l'exposition au risque, l'organisation peut être amenée à modifier l'activité économique et sociale qui utilise le numérique. Par exemple, la prise de décision de concevoir certaines fonctionnalités différemment afin de réduire le risque dans un produit – décision économique s'il en est – peut impacter sa position sur le marché, son prix etc. Preuve supplémentaire que la gestion de risque numérique doit être partie intégrante de la décision économique.

Chaque fois qu'une décision d'utiliser le numérique pour développer l'activité économique est prise, c'est dans la perspective d'un bénéfice. On doit donc gérer le risque dès qu'on envisage d'utiliser le numérique, et ce sont les mêmes décideurs qui doivent gérer les opportunités et les risques, car les deux sont indissolublement liés.

Les principes de la Recommandation ont pour objectif de permettre aux entreprises et organisations de mettre en place des politiques internes pour faire le lien entre leur cadre de gestion de risque, si elles en ont un, et la question du risque numérique, afin de l'intégrer au cadre général existant.

La seconde partie de la Recommandation concerne les stratégies nationales et contient une trentaine de recommandations. Parmi elles, notamment l'impératif pour les stratégies nationales d'être soutenues au plus haut niveau de l'Etat. L'idée étant alors de coordonner les différents acteurs pour avoir une vision la plus englobante possible, rassemblant les questions économiques et sociales, de sécurité nationale et internationale, ou encore de lutte contre la cybercriminalité ».

Désormais, l'OCDE doit suivre la mise en œuvre de cette Recommandation par les Etats. Elle travaillera également sur d'autres sujets connexes, telles que la mise en œuvre de la gestion de risque de sécurité numérique par les individus et les petites entreprises, ou encore les questions liées à l'assurance.

- **Questions-réponses :**

Benoît Moreau, FSSI du ministère de l'Education nationale
Les risques politiques instantanés sont-ils abordés dans la Recommandation ?

Laurent Bernat
Dès que la décision d'avoir recours au numérique pour une activité économique est envisagée, qu'il s'agisse d'un produit, d'un service, ou d'une des étapes de la chaîne de valeur, on doit commencer à gérer les risques numériques correspondants. Si on vise un bénéfice, on doit gérer les risques pour augmenter les chances de l'atteindre et réduire les probabilités de conséquences négatives.
Le document d'accompagnement de la Recommandation explique ces concepts, l'idée étant de dire que l'opportunité et le risque sont liés et sont les deux faces de l'innovation.

Emmanuelle Diolot, Société Générale
La Recommandation précise-t-elle comment s'organisent les choses au niveau des entreprises ?

Laurent Bernat
Elle n'entre pas dans le détail, mais elle fixe les grands principes. Au plan opérationnel, on peut avoir recours à des normes pour la mettre en œuvre. La Recommandation s'adresse d'abord aux dirigeants. Pour le détail, tout dépend de l'organisation de l'entreprise. La Recommandation ne dit pas qui doit faire quoi, car cela dépend de la culture d'entreprise et de beaucoup d'autres facteurs. Elle dit qu'il

faut qu'il y ait un plan pour gérer les risques lorsqu'ils se réaliseront. Les processus sont propres à chaque entreprise. Le risque numérique étant un risque comme les autres, les entreprises doivent l'intégrer à leur cadre général de gestion de risque. Cela pose par ailleurs la question de la gouvernance du risque numérique, et notamment des compétences et de la position dans l'organigramme du RSSI : doit-il être uniquement un expert technique ou doit-il avoir conscience des enjeux économiques et sociaux de l'entreprise ? Quelle doit-être sa responsabilité ? A qui doit-il rendre compte ?

Il faut distinguer ce qui est financier et ce qui ne l'est pas. Les coûts économiques et sociaux sont difficiles à calculer et non réductibles. Est-ce que le chef d'entreprise ne devrait pas gérer la mise en conformité à des exigences ?

Laurent Bernat
La question de la conformité est importante et fait partie de la Recommandation. Quand les menaces sont élevées et mal gérées par les acteurs économiques, le législateur veut naturellement imposer des règles. Mais il faut faire attention car la création d'obligations augmente la rigidité et limite la flexibilité. Or, la rigidité est en contradiction avec l'environnement numérique. La conformité est parfois nécessaire, mais il ne faut pas que cela inhibe l'innovation. Pour cela, l'OCDE prône la coopération entre les parties prenantes. L'Etat, les régulateurs, le législateur, les entreprises, doivent coopération pour bien comprendre les réalités économiques, techniques, et autres auxquelles les organisations font face.
La conformité est parfois nécessaire mais il doit y avoir une réflexion en amont sur comment la concevoir et la mettre en œuvre. Par ailleurs, elle n'est pas considérée de la même manière selon les pays : cela dépend de la culture. Par exemple, en France, on aime bien la règlementation tandis qu'en Grande-Bretagne, à l'inverse, on la fuit. C'est très culturel.
La question des normes que peuvent imposer les grandes entreprises aux PME est également au cœur du problème. L'implication des différents acteurs dans les processus de développement des normes est stratégique : la PME ne peut pas inventer une norme mais si elle existe et qu'elle a été développée de façon réaliste, en tenant compte des contraintes d'une petite structure, elle pourra l'appliquer. La condition *in fine* est que la norme soit claire, précise et flexible, de sorte que les PME puissent aussi s'y conformer.

Diane Rambaldini, Crossing Skills
Les prestataires sont les premiers freins à la Recommandation. Celle-ci ne devrait-elle pas d'abord s'adresser à eux ? L'approche de sécurité est rare chez les prestataires, qui différencient le « risk management » de la gestion du risque cyber.

Laurent Bernat
Plusieurs représentants du secteur privé ont participé aux réflexions sur la Recommandation de l'OCDE, notamment des représentants du secteur des TIC. Leurs clients sont les directions informatiques et non pas les directions métiers donc ils vendent de la « sécurité » aux premiers, plus que de la gestion de risque économique. Les fournisseurs de solutions techniques sont là pour apporter des mesures de sécurité techniques, il n'est donc pas étonnant qu'ils soient assez peu orientés vers le risque économique. Mais ceux qui apportent du conseil intègrent davantage le « *risk management* » car ils ont un meilleur accès aux directions métier.

Philippe Hubert, ANSSI
Est-il possible de dresser un panorama sur la maturité des Etats membres de l'OCDE sur ce sujet ?

Laurent Bernat
Une étude comparative des stratégies nationales de cybersécurité est sortie en 2012 car l'OCDE avait identifié l'émergence d'une nouvelle génération de stratégies. Sept ou huit pays se sont portés

volontaires pour cette étude, dont la France. Le rapport issu de cette étude est intéressant mais désormais peut-être un peu daté.
Pour faire un comparatif, il y a deux méthodes : l'étude des données quantitatives et celle de données qualitatives. L'étude quantitative est délicate dans ce domaine : on ne peut calculer l'impact d'une stratégie nationale pour exemple, surtout en l'absence d'indicateurs quantitatifs robustes et comparables internationalement. Ce sont donc les données qualitatives qui importent, et donc l'analyse des stratégies nationales en elles-mêmes ainsi que des mesures de mise en œuvre. C'est ce que nous ferons régulièrement désormais pour savoir comment ils appliquent la Recommandation, lesquels sont les plus actifs, lesquels ont les mesures les plus originales. L'objectif sera moins d'évaluer les meilleurs que d'aider à partager les bonnes pratiques.
Il est possible de dire que la nouvelle stratégie française est assez en phase, à la pointe, par rapport à d'autres membres de l'OCDE, notamment parce que c'est la plus récente, mais aussi parce qu'elle prend en compte le paradigme économique sans pour autant oublier les autres dimensions.
Ceci étant, la stratégique britannique de 2011, en comparaison, avait pour slogan « Faire de la Grande Bretagne le meilleur endroit pour faire du business ». Ce leitmotiv a donné lieu à des initiatives intéressantes, notamment eu égard au partenariat public-privé. Le rapport entre l'Etat et l'économie est également une question culturelle.
En conclusion, chaque pays a ses propres forces et ses faiblesses, il est donc difficile de les casser, mais il est utile de les comparer pour s'enrichir mutuellement.

Pour nous contacter
Tél : 09 83 04 05 37
contact@cybercercle.com