



Monsieur le Ministre de l'Economie, des Finances et de la Réforme de l'Administration,
Monsieur le Ministre de l'Industrie, du Commerce et de l'Economie Verte et Numérique,
Monsieur le Président de la Commission Nationale de Contrôle de Protection des Données à Caractère Personnel,
Mesdames et Messieurs, Honorable assistance.

C'est pour moi un honneur et un plaisir d'être parmi vous en cette occasion devenue un rendez-vous annuel incontournable d'information et de sensibilisation sur la cybersécurité, organisé par la DGSSI.

Cet espace de dialogue et d'échange entre responsables et experts cyber de tous horizons nous offre cette année l'occasion de placer au centre de nos discussions une thématique aussi importante qu'actuelle, en l'occurrence celle des enjeux de la cybersécurité dans le cadre des projets d'externalisation des systèmes d'information.

Je voudrais, en cette circonstance, remercier chaleureusement Messieurs les Ministres et Monsieur le Président de la CNDP d'avoir bien voulu nous honorer de leur présence à ce séminaire et de partager avec nous leurs réflexions et orientations pertinentes au sujet de l'externalisation IT.

Je souhaite aussi la bienvenue aux participants qui ont bien voulu témoigner aujourd'hui l'intérêt qu'accordent nos organismes publics et privés aux différentes manifestations organisées par la DGSSI.

Permettez-moi également de remercier vivement et saluer chaleureusement nos honorables invités, qui ont bien voulu partager avec nous leurs expériences dans le domaine de l'externalisation des Systèmes d'Information.

Ma sincère gratitude va ensuite aux experts intervenants qui ont eu l'obligeance de prendre part aujourd'hui à cette manifestation et échanger avec les participants, leurs connaissances et leurs expériences dans le cadre de cette thématique.

Nous souhaitons, par le biais de ce rassemblement de tant de compétences et d'expériences, développer la coopération et concrétiser les complémentarités à travers le partage des retours d'expériences nationales et internationales dans le domaine de la cybersécurité et de l'externalisation des Systèmes d'Information.

Mesdames et Messieurs,

L'externalisation des systèmes d'information est un phénomène en constante évolution qui concerne désormais bon nombre de secteurs d'activités et se présente comme une tendance durable et irréversible. Autrefois apanage des grandes entreprises industrielles et du secteur financier, la sous-traitance informatique suscite désormais un intérêt certain chez des acteurs économiques de toute taille et notamment auprès d'entités publiques de plus en plus enclines à confier à des partenaires extérieurs la réalisation de tout ou partie des activités qu'elle réalisait préalablement en interne. D'aucuns estiment, dans ce cadre, que le marché global du Cloud public devrait atteindre **380 MM** de dollars en 2020 contre 250 MM de dollars environs en 2017, soit un taux d'accroissement annuel de plus de 13%.

Le recours à la démarche d'externalisation des SI offre des avantages importants en termes d'accessibilité et d'élasticité. Les ressources externalisées demeurent accessibles sur tous les supports via une connexion internet. Cet avantage indéniable pour les organisations vient se conjuguer avec celui de la souplesse d'emploi qui permet une allocation optimale et adaptée des ressources en fonction des besoins de l'organisation.

Par ailleurs, les objectifs d'amélioration constante de la performance et des résultats encouragent les managers à recentrer et focaliser leurs activités sur leur cœur de métier. Dans ce cadre, les fonctions à qualifications particulières, notamment celles liées aux SI, sont externalisées pour profiter de compétences nouvelles et s'ouvrir sur des solutions technologiques en phase avec les besoins de l'organisation ou encore pour sécuriser ce SI notamment lorsqu'il s'agit de petites structures à potentiel limité dans ce domaine.

Enfin, les acteurs publics et privés sont de plus en plus attentifs à la réduction des coûts d'investissement et de fonctionnement de leurs systèmes d'information. Ces systèmes, qui deviennent de plus en plus étendus et complexes, mobilisent des ressources humaines importantes et nécessitent des efforts financiers considérables pour en supporter les coûts d'acquisition, de maintenance des équipements, logiciels et de formation de personnels techniques. Le recours à l'externalisation paraît, dès lors, comme une solution viable et optimale pour répondre à ces exigences.

=====

Devant ces opportunités et avantages, les responsables seraient confortés dans leurs décisions de recours à l'externalisation de leurs SI. Cette optique nécessite, toutefois, la prise en compte et la maîtrise de certains risques juridiques, techniques et de sécurité que je survolerai brièvement :

D'abord et d'un point de vue juridique, se pose la question de la réglementation applicable à l'externalisation des systèmes d'information.

Il s'agit de mettre en place un cadre réglementaire cohérent, qui garantit la confidentialité, la protection des données personnelles ou sensibles et le respect de leur intégrité. Le contrat conclu dans le cadre du Cloud doit contenir des clauses de responsabilité particulièrement en matière de respect de confidentialité et de sécurité des données attendus par l'organisation tout au long de la durée de vie du contrat.

Sur ce plan, se pose également la question de la territorialité en ce qui concerne la localisation des données. Ce principe de territorialité renvoie à la nécessité de pouvoir constater à tout moment, la localisation des données externalisées.

La localisation des données pose aussi le problème de la compétence des juridictions et du droit applicable, ce qui appelle une étude approfondie des conditions des offres d'hébergement des données, en particulier le régime juridique auquel ces dernières sont soumises et les mesures mises en œuvre pour en assurer la confidentialité.

2. Ensuite, sur le plan technico-opérationnel, les organisations se doivent d’œuvrer constamment à maintenir un niveau de maîtrise adapté sur leurs système d’information.

En effet, le recours à l’externalisation sans mesures d’accompagnement appropriées pourrait, dans certaines situations, impacter le contrôle de l’activité et éventuellement induire une perte du savoir- faire en interne.

En utilisant les services du Cloud, l’organisation pourrait concéder au prestataire un contrôle total sur son SI. Ceci induirait une forme de dépendance technologique vis-à-vis du prestataire.

3. Enfin, et s’agissant de la sécurité des systèmes d’information externalisés, une attention particulière doit être accordée à la nature des données à externaliser.

Afin d’éviter toute éventuelle divulgation d’informations générée par une externalisation non maîtrisée, les entités publiques ou privées doivent procéder à une classification de leurs données en fonction de l’analyse des risques et ceci afin d’opter pour le mode le plus adapté.

Elles doivent, de même, veiller à la mise en place de mesures nécessaires pour éluder les risques induits par la mutualisation des infrastructures.

La vigilance doit aussi et surtout être de mise en matière de gestion des accès à distance au système d’information qui peuvent constituer une source de vulnérabilité et un point d’entrée potentiel d’actions malveillantes.

=====

Mesdames et Messieurs,

La sécurité n’est antinomique à l’externalisation, cependant concilier externalisation et sécurité soulève de nombreuses interrogations auxquelles les responsables des SI, à tous les niveaux, doivent apporter des réponses adaptées. Vous avez aujourd’hui une opportunité pour apporter des éclairages utiles à ces questions.

Il est en effet indispensable de prendre en compte les préoccupations légitimes des utilisateurs, liées à la conformité aux dispositions légales et réglementaires, la maîtrise des risques et l’adéquation des mesures techniques adaptées à la sécurité des données à externaliser.

La prise de décision en matière d’externalisation restera tributaire de la capacité à offrir un niveau de garantie soutenable pour répondre au souci permanent des décideurs, celui de favoriser un fonctionnement optimal de leurs structures tout en assurant une meilleure protection de leur patrimoine informationnel.

Dans ce sens, on peut faire référence à la possibilité de développement **d’installations souveraines** et d’une **offre nationale** qu’il convient d’encourager. Ceci permettra non seulement de satisfaire aux besoins des organismes nationaux et la maîtrise des enjeux de cybersécurité, mais aussi d’ériger le Maroc en plate-forme internationale d’IT Outsourcing pour ainsi enrichir son écosystème économique numérique.

Mesdames et Messieurs,

Je souligne que la 7^{ème} édition de notre séminaire sur la cybersécurité, tentera d'apporter des éléments de réponses susceptibles d'aider à la maîtrise des problématiques liées à l'externalisation notamment au sein des administrations, organismes publics et infrastructures d'importance vitale publiques et privées.

Je ne pourrais laisser passer l'occasion sans évoquer devant vous **certaines actions réalisées par la DGSSI**, dans le cadre du renforcement de la cybersécurité au Maroc. Je me limiterai à ce titre à trois actions majeures :

La première concerne la mise à niveau de notre arsenal juridique à travers la mise en place d'une Loi cyber, dont le projet est actuellement en cours d'examen et de finalisation en concertation avec les départements et organismes concernés. Cette loi consacre des dispositions auxquelles seront soumis les prestataires de services numériques notamment ceux qui fournissent des services liés à l'externalisation des données.

La seconde porte sur le projet de loi relative aux services de confiance pour les transactions électroniques. Ce projet a pour but notamment de consolider la confiance numérique dans notre pays à travers notamment la signature électronique, la sécurisation des accès à distance, sources de vulnérabilité et d'actions malveillantes.

La troisième concerne les actions entreprises par la DGSSI dans le but d'aider les organismes nationaux dans la prise de décision liée à l'externalisation de leurs SI. Plusieurs guides et référentiels comme « *le guide d'externalisation des systèmes d'information* », « *le guide de gestion des risques de sécurité SI* » ou encore « *le référentiel de classification des SI* » ont été élaborés et publiés par les services de la DGSSI au cours des dernières années. Ces guides sont actuellement en phase de mise à jour pour intégrer les nouvelles tendances en la matière.

Avant de conclure, je réitère mes sincères remerciements à Messieurs les Ministres et Monsieur le Président pour leur participation à cette séance inaugurale.

Je ne saurais terminer mon propos sans remercier les organisateurs de ce séminaire et Bank Al Maghrib qui a eu l'amabilité de mettre à notre disposition une fois de plus des infrastructures d'accueil de qualité pour l'organisation de ce séminaire.

Mes remerciements vont également aux participants et experts présents parmi nous, merci à vous tous pour votre attention et votre intérêt.

Je souhaite que vos travaux soient enrichissants et fructueux.