



Commission économique pour l'Afrique



Union du Maghreb Arabe

Aide-mémoire

Atelier sur l'harmonisation de la cyberléislation au Maghreb

Rabat, 9-11 mai 2012

Les sociétés d'Afrique comme celles dans d'autres parties du monde, dépendent de plus en plus des technologies de l'information et de communication, et sont donc vulnérables aux menaces sur le cyber espace telles que la cybercriminalité.

Les criminels, les groupes du crime organisé et les terroristes recourent en effet de plus en plus au potentiel des TIC pour faciliter leurs crimes. En attendant, les consommateurs hésitent à transmettre des données personnelles et à effectuer des transactions sur le net, la sécurité et la confidentialité étant leurs préoccupations majeures. De même, les entreprises subissent des pertes importantes de données propriétaires, la propriété intellectuelle et l'accès en ligne aux clients et fournisseurs en raison de failles de sécurité.

Sans des lois pénales et règlements appropriés, ainsi que la capacité d'application de ces lois, d'enquêter et de coopérer au plan international, les économies peuvent devenir attractives comme des paradis et des centres de blanchiment d'argent pour les criminels et les activités terroristes.

Pour que les TIC puissent contribuer à la croissance économique, au développement humain, et la démocratisation, elles doivent être fiables et sécurisées. Un manque de confiance et de sécurité compromet de nombreux développements qui pourraient être soutenus par une économie du savoir largement accessible, et qui bénéficie pleinement de la confiance de la société. Les enjeux portent notamment sur :

- La croissance du e-commerce entre les entreprises et entre entreprises et consommateurs.
- L'attraction des investissements étrangers nécessaires à la création d'entreprise, la modernisation des infrastructures et l'innovation qui sont aussi tributaires des systèmes juridiques et sont sensibles aux problèmes de sécurité informatique.
- L'e-gouvernement et les efforts visant à rendre le gouvernement plus réactif et plus accessible sont menacés par des problèmes de sécurité et de la crainte d'abus.
- La création d'emplois et le développement de «services back-office» par les entreprises mondiales qui cherchent des coûts salariaux plus bas pour la saisie et le traitement des données, seront freinés dans les pays sans lois sur la protection des données à caractère personnel.
- La sécurité des infrastructures essentielles pour la production et la distribution d'énergie, les transports, banques, et les opérations de soins de santé sont de plus en plus dépendants des systèmes d'information.

- La protection de la vie privée, les données personnelles, les communications et les données stockées sur les entreprises et les individus doivent être protégés à la fois contre l'interception illégale, et contre l'accès et la surveillance arbitraire.
- Les centres de développement des soins, de la télémédecine et la santé dans lesquels les utilisateurs ne feront pas confiance en ce qui concerne leurs informations médicales, dans un milieu précaire de communications.
- L'utilisation des technologies de l'information pour l'apprentissage à distance, les services de recherche d'emploi, l'amélioration des compétences, et le développement des petites et moyennes entreprises.
- Au vu de ces enjeux, la CEA a reconnu la nécessité de relever le défi de la cybersécurité au niveau national sous-régional et régional.
- Dans ce contexte, le bureau de la CEA pour l'Afrique du Nord, la division des TIC et des Science et Technologies (ISTD) en collaboration avec le Conseil de l'Europe (COE), Microsoft et le CNRST, ont organisé en Juillet 2010 à Rabat, un atelier sur l'harmonisation du cadre légal pour le cyber sécurité en Afrique du Nord. L'atelier a permis, entre autre, l'identification des besoins pour une réforme de la cyber législation dans la région.

En guise de suivi, la CEA organise en collaboration avec le Secrétariat Général de l'Union du Maghreb Arabe (UMA), un atelier sur l'harmonisation de la cyber législation au Maghreb, avec un accent particulier sur l'examen et la discussion du projet de lignes directrices sous régionales pour la cyber sécurité.

Objectifs

L'objectif de l'atelier est de soutenir le renforcement de la cyber législation dans les pays du Maghreb en conformité avec les normes internationales. Il vise à aider les pays du Maghreb à respecter leurs engagements vis-à-vis du Sommet mondial sur la Société de l'information (SMSI), et pour ce, s'efforcer d'adopter des cadres juridiques pour renforcer la cybersécurité et la confiance dans la société de l'information et l'économie du savoir. L'atelier permettra également d'aider les participants à mieux rédiger des législations sur la cybercriminalité, les transactions électroniques, et la protection des données personnelles en harmonie avec ce qui se fait à l'échelle internationale et régionale.

Les participants

Les délégations comprennent des experts en cyberlégislation des départements des TIC, de la justice, du Commerce, d'application de la loi, les décideurs, y compris des experts des organes législatifs, les tribunaux et les universités.

Langue de travail : Arabe et Français

Lieu: Centre National pour la recherche Scientifique et Technique (CNRST)
Angle Av. Allal Al Fassi et Av. des FAR Hay Ryad Rabat – Maroc
Tél.: +212 537 5698 12 - Fax: +212 537 56 98 11

Date : 9-11 mai 2012