

La confiance numérique au Maroc

Il appartient à l'Etat d'établir la confiance numérique et de garantir la sécurité dans le cyberspace. La tâche est plus ardue qu'il en paraît puisqu'il est difficile de contrôler humainement et techniquement un Internet sans frontière. Au Maroc, à défaut d'un texte fondateur décrivant la stratégie, tout comme la vision globale, à mettre en place pour sécuriser le cyberspace marocain, nos politiques ont entrepris différentes actions à plus ou moins grande échelle. Parmi ces initiatives, le programme «Confiance numérique» prévu dans le cadre de la stratégie «Maroc Numeric 2013», est incontestablement la feuille de route la mieux élaborée à l'heure où nous écrivons ces lignes. Cependant, malgré son caractère transverse, le programme représente des limites sérieuses à l'instauration d'une véritable confiance numérique.

Le renforcement du cadre législatif

Que ce soit la loi n°07-03 complétant le Code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé des données, la loi n°53-05 relative à l'échange électronique de données juridiques ou la loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, le Maroc est en train de réaliser des efforts certains pour mettre à niveau son arsenal législatif. Toutefois, le manque de jurisprudence et de définitions communes entre le technicien et le magistrat sont autant des limites à la mise en place d'une réelle politique judiciaire de répression de la cybercriminalité. Durant les prochaines années, le Maroc sera devant un enjeu stratégique. Il s'agit de l'interprétation des impacts juridiques que peuvent avoir les infractions informatiques compte tenu de leur complexité. Pour le relever, l'Etat doit créer plus de passerelles entre l'univers informatique et celui des juristes

comprenant aussi bien des avocats, des magistrats que des policiers et des gendarmes. La formation en est un axe capital. En effet, pour pouvoir appliquer la loi, il s'avère indispensable, notamment pour les magistrats et avocats, de se mettre à niveau en matière de la cybercriminalité.

Mise en place des structures organisationnelles appropriées

Les ripostes juridiques en matière de lutte contre la cybercriminalité, aussi exhaustives soient-elles, seront insuffisantes si elles ne sont pas accompagnées par la mise en place d'institutions chargées notamment de répression, d'investigation et de veille en matière de cybercriminalité. Dans cette perspective, le programme «Confiance numérique» a eu le mérite de prévoir la mise en place de nombreux organismes (CSSI, ma-CERT, tiers de confiance, CNDP, etc.).

Le Comité de sécurité des systèmes d'informations (CSSI)

Cette initiative, bien que louable, reste insuffisante. En effet, par définition un comité ne propose que des actions ponctuelles. Or, pour pouvoir piloter la confiance numérique, il faut un travail structurel. Pour y parvenir, de nombreux pays ont mis en place des Agences nationales de sécurité des systèmes d'information (ANSSI). C'est le cas par exemple de la France, du Canada mais aussi de la Tunisie.

Le centre de veille ma-CERT

Pour assurer une meilleure veille en matière de sécurité et coordonner ainsi les réponses aux incidents liés à la sécurité des systèmes d'information, ma-CERT au niveau national, un centre dédié, sera mis en place dans les prochains mois. Précisons cependant, que le centre ne disposera pas d'une plateforme de signalement qui permettra aux internautes marocains

de signaler les sites illicites tels que les sites pédopornographiques, les sites d'incitations à la haine, aux injures raciales, au terrorisme et de déclarer les incidents cybercriminels à l'image de ce qui se fait par exemple en France. Ce dispositif, permettra d'élucider les délits et les orienter vers les services de polices, de gendarmerie et des douanes et éventuellement vers Interpol. Il sera pris en charge en partie par le portail de la sécurité des systèmes d'information proposé par le DEPTI (Département de la poste, des télécommunications et des nouvelles technologies au Maroc).

Promotion d'une culture de sécurité

L'être humain est le maillon faible de la chaîne de la sécurité. De nombreuses techniques cybercriminelles s'appuient sur ce constat. De ce fait, quelles que soient les mesures de sécurité mises en place, elles n'auront du sens que si elles sont accompagnées par la promotion d'une véritable culture de sécurité. Il s'avère donc important de développer, traiter et soutenir cette culture de sécurité au niveau de toutes les couches de la société.

Les campagnes de sensibilisation

Quelle que soit la cible envisagée, les campagnes de sensibilisation doivent s'inspirer, pour une meilleure efficacité, du modèle des campagnes destinées à favoriser l'usage de la ceinture de sécurité au volant. Une telle démarche permettra de sous tirer des utilisateurs en ligne, un comportement sécurisé et respectueux de la légalité. Comme pour la ceinture de sécurité, un effort d'éducation à long terme est nécessaire pour que de telles mesures aient de l'effet.

La formation

La promotion de la culture de sécurité passe aussi par la mise en place des formations à destination des étudiants de l'enseignement supérieur.