Ce mercredi 02 Septembre 2020, à l'hôtel *Les Résidences Mamoune*, s'est tenu un « ATELIER AVEC LES JOURNALISTES ET AUTRES ACTEURS DES MÉDIAS SUR LES ENJEUX ET PRATIQUES DE LA GOUVERNANCE DE LA CYBERSÉCURITÉ DU SENAGAL », organisé par l'Organisation JONCTION en partenariat avec GLOBAL PARTNERS, entre 15h49 et 19h.

Cette rencontre qui a vu la participation de plusieurs acteurs des médias et d'organisations de la société civile et sous la présidence du Ministère de l'Économie Numérique et des Télécommunications, représenté par le Directeur des TIC.

Il a été l'occasion d'échanger et de partager avec les participants sur l'état des lieux de la mise en œuvre de la stratégie nationale de cybersécurité. Mais spécifiquement, l'atelier vise à *sensibiliser les journalistes et autres acteurs des médias sur les instruments pertinents de protection du droit de l'homme relatifs à la cybersécurité ; échanger sur la vision du gouvernement en matière de cybersécurité ; donner un aperçu global sur la mise en œuvre de la stratégie nationale de cybersécurité adoptée par le gouvernement du Sénégal ; échanger sur les différents enjeux, défis, et thèmes d'actualité dans le domaine de la cybersécurité ; identifier les défis et obstacles pour une mise en œuvre efficace de la stratégie nationale de cybersécurité.*

Pour ce faire, deux thèmes ont été animés avec la modération de M. El Hadji Daouda DIAGNE, Spécialiste en cybersécurité, Directeur de Camputech Institute. La séance a démarré après le mot de bienvenue de M. DIOP, Président de JONCTION, qui est revenu sur le contexte de cet atelier.

Le premier portant sur les « *Enjeux et pratiques de la gouvernance de la cybersécurité au Sénégal : quel rôle pour les parties prenantes dans la protection des droits de l'homme* » est développé par M. Justin Oumar Bamah Ossivi, juriste –chercheur.

Dans son exposé, le panéliste relevé l'impact voir la place de l'univers numérique aussi bien dans le quotidien des uns et des autres mais également dans la vie économique du pays. Cela a fait qu'aujourd'hui le Sénégal a adopté une stratégie nationale sur la cybersécurité arrimée au Plan Sénégal Émergeant (PSE) et dont le slogan est : « le numérique pour tous et pour tous les usages en 2025 au Sénégal avec un secteur privé dynamique et innovant dans un écosystème performant ».

Par ailleurs, la digitalisation implique l'existence d'un espace fiable et sécurisé. L'atteinte de cet idéal doit être une affaire de tous ; aussi bien des pouvoirs publics que des utilisateurs. Mais

quoi qu'il en soit, la problématique du respect des droits humains doit être prise en compte, effective dans la lutte contre la cybersécurité.

La notion de *cybersécurité* relève-t-il d'ailleurs, fait l'objet de diverses définitions. Il y a par exemple celle retenue par la SNC 2022 qui met l'accent sur les mesures de protection contre les menaces et les attaques ; les mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels et la lutte contre la cybercriminalité. Non s'en se réjouir de constater cette dimension des droits de l'Homme soit apparue dans la définition même retenue par le groupe de travail de la FOC (freedom online coalition) dont il trouve « plus protectrice des droits fondamentaux que celle de la SNC, parce qu'elle place les droits humains au cœur de la cybersécurité. Selon FOC, la cybersécurité renvoie à la préservation par la politique, la technologie l'éducation, la disponibilité, la confidentialité et de l'intégrité des informations et de leurs infrastructures sous-jacente afin d'améliorer la sécurité des personnes en ligne et hors ligne. »

Ce cadre a été l'occasion de revenir également sur des questions aussi essentielles que la souveraineté numérique ; le nécessaire équilibre à trouver entre la sécurité et la liberté. Cette dernière préoccupation suscite un questionnement sur l'importance des droits humains dans la gouvernance de la cybersécurité. Elle se mesure à plusieurs niveaux. En effet, « la plupart des risque et menaces qui pèsent sur la cybersécurité peuvent avoir des conséquences sur les droits de l'homme. » Par exemple : le déni de fourniture d'information ; la fermeture du réseau ; la restriction d'accès à l'information (internet) ; les fuites des données ; la surveillance de masse ; etc.

Au terme de sa réflexion, le panéliste a recommandé de faciliter l'adaptabilité des instruments de gouvernance sécuritaire de l'écosystème numérique ; créer un Certification de sécurité numérique par la CERT national ; élaborer une charte de bonne cybergouvernance sécuritaire ; amplifier les concertations sur la sécurité numérique entre acteurs de la société civile et pouvoirs publics ; inclure des programmes d'enseignement et de capacitation de culture numérique au cœur de nos programmes d'éducation ; promouvoir une cellule de veille permanente des droits numériques.

Le deuxième portant sur état des lieux de la stratégie nationale de cybersécurité a été présenté par M. Achime Malick Ndiaye, Directeur des TIC au Ministère de l'économie numérique et des télécommunications. Dans sa communication, il a relève avec regret la passiveté citoyenne qui consiste à rester statique, fuir ses responsabilités, rejeter la faute sur les autres alors même qu'on s'est abstenu d'agir, de nous impliquer dans un processus. C'est un problème comportemental culturel à révisier fort bien déplorable.

Or, aujourd'hui la démarche de l'État c'est d'impliquer tout le monde dans les processus. C'est en ce titre que dans l'élaboration de la SNC 2022, tous les acteurs ont été impliqués ; ce qui a permis de trouver un cadre consensuel. Cette méthode est adoptée aux fins de favoriser l'implication, l'appropriation citoyenne.

Sur le terrain et de façon pratique, des efforts et des réalisations se font en vue de lutter contre la cybercriminalité. On peut faire référence à la formation des agents de police ; la création d'une école nationale de cybersécurité à vocation régionale ; l'obligation pour les banques d'établir un certificat de conformité de leurs équipements, de leurs infrastructures numériques afin de permettre de veiller à la sécurité des transactions.

En outre, aujourd'hui le défi de la gouvernance de la cybersécurité pose problème du fait de la pluridisciplinarité des acteurs spécialisés sur les questions de cybersécurité alors même qu'il n'y a pas de cadre devant les rassembler. Aussi, la révision des lois sur la sécurité de l'information constitue une question essentielle dont le plaidoyer est relatif aussi bien sur l'application que le respect des normes ; car tant que cet idéal n'est pas atteint, les textes, aussi pertinents soient-ils, ne seront d'aucune efficacité.

Dakar le, 02 Septembre 2020

Rédigé par ***M. DIÉMÉ Simon***

Récépissé N° : 12 530 / MINT.CL/DAGAT/DEL/AS
Siège Social : BP : HLM Grand Médine n° 287 BP : 4126 Dakar-Sénégal
Tel : (221) 77645 42 46 fax : (221) 338252861 Email : jonction_jonction@yahoo.fr
Web : http://jonction.e-monsite.com/