Cybersécurité et Lutte Nationale contre la Corruption

Le juge. Hatem Gaafar

Expert en cybersécurité et en preuves numériques à l'Union internationale des télécommunications

La prise de conscience mondiale de l'importance de la cybersécurité s'est accrue ces dernières années en raison de l'énorme développement de la manière dont la technologie est utilisée et de la qualité de cette utilisation, ce qui a conduit à l'inévitabilité du recours à ces nouveaux moyens, à l'émergence du terme transformation numérique et à l'augmentation du pourcentage de dépendance à l'égard de ces moyens.

De plus, le besoin urgent d'étendre cette transformation numérique est devenu évident avec l'avènement et la propagation de la pandémie de corona dans le monde, qui a transformé la question d'un choix et d'un luxe en un mode de vie et un impératif indispensable et irremplaçable, ce qui a conduit à la diffusion de la transformation numérique en Égypte en raison de ses nombreux avantages, notamment le gain de temps, d'efforts et d'argent, la facilité de fournir des services aux citoyens et de leur permettre de bénéficier de ce développement, conformément à la Vision 2030 de l›Égypte, et cela impliquait la nécessité de sécuriser les transactions résultant de la transformation numérique dans un cadre cohérent et harmonieux avec le reste des efforts de l›État afin de prévenir et combattre la corruption dans cet environnement technologique, avec ses nouveaux mécanismes et méthodes avancées de corruption et la nécessité de moyens de prévention et de contrôle plus sophistiqués .

L'Égypte s'est très tôt intéressée au domaine de la cybersécurité et a cherché à diriger la scène arabe et africaine dans les indicateurs internationaux , et était également à l›avant-garde des pays visant une amélioration continue et créant une expérience réussie et pionnière au Moyen-Orient. Par conséquent, l'Egypte a atteint la neuvième place au niveau mondial dans l'indice mondial de la cybersécurité «GCI» pour 2014, et sous la gouvernance de la cybersécurité au niveau national, l'Égypte a publié la stratégie nationale pour la cybersécurité 2017-2021 conformément aux tendances mondiales modernes et aux droits contenus dans la Constitution égyptienne publiée en 2014 à l'article 31 qui stipule : « La cybersécurité est un élément essentiel du système d'économie et de sécurité nationale, et l'État s'engage à prendre les mesures nécessaires pour la préserver, conformément à la Loi «.

D'autre part, l'Égypte a cherché à construire et à établir un système moderne capable de protéger le cyberespace égyptien, en créant le Conseil suprême de la cybersécurité dirigé par le ministre des Communications et des Technologies de l'information. Le Conseil comprend des représentants du gouvernement, du secteur privé et de la société civile ainsi qu'un représentant de l'Autorité de Contrôle Administratif. Le Conseil vise à renforcer la cybersécurité en Égypte et à protéger les infrastructures critiques du gouvernement et du secteur privé contre d'éventuelles cyberattaques .

Le Conseil a pris de nombreuses décisions organisationnelles pour atteindre cet objectif, notamment le développement des capacités nationales en matière de cybersécurité, le renforcement de la coopération internationale dans ce domaine, en plus de superviser la mise en œuvre de la Stratégie nationale de cybersécurité.

Aborder le rôle de la cybersécurité dans la Lutte contre la Corruption nécessite l'affirmation que la Corruption est un phénomène social, politique et économique qui menace l'ordre public, la sécurité nationale et le développement durable des États, et peut être définie comme «la déviation ou la destruction des fonctions publiques par la concussion et le népotisme» ainsi que «les actions malhonnêtes menées par des personnes occupant une position de pouvoir pour un gain privé ou un abus des ressources disponibles».

La cybersécurité telle que définie par l'UIT est «l'ensemble des outils, politiques, directives, approches de gestion des risques, procédures, formations, meilleures pratiques, mécanismes d'assurance et technologies qui peuvent être utilisés pour protéger la disponibilité, l'intégrité et la confidentialité des actifs dans les infrastructures connectées des gouvernements, des organisations privées et des citoyens, ces actifs comprennent les appareils informatiques connectés, le personnel, l'infrastructure, les applications et services, les systèmes de communication et les données dans le cyberenvironnement».

L'une des formes les plus dangereuses de cybercriminalité est celle qui cible les secteurs gouvernementaux, en particulier ceux chargés de lutter contre la Corruption. Ces secteurs ont besoin d'une protection élevée de leurs données et systèmes contre toute interférence externe visant à affecter leur processus de travail, à divulguer des informations confidentielles, à modifier les résultats des enquêtes, à les discréditer ou à perturber leurs services. Ces mesures sont le nerf de la cybersécurité visant à atteindre trois objectifs principaux, à savoir :

La confidentialité qui consiste à empêcher l'accès aux informations sauf aux personnes autorisées et à déterminer qui a le pouvoir de les modifier, de les supprimer ou de les ajouter.

L'Intégrité qui est une garantie de l'exactitude et de l'intégrité des informations lorsqu'elles sont saisies, enregistrées ou transmises dans le système.

La disponibilité qui est une garantie d'accès à l'information à tout moment et qu'elle ne sera pas perturbée.

Compromettre l'un des éléments ci-dessus constitue une violation des procédures de cybersécurité.

Si nous prenons en compte la définition précédente de la cybersécurité et de ses composantes et la définition de la corruption, nous constatons que la cybersécurité est le dispositif de lutte contre la corruption des systèmes automatisés et de leurs bases de données après la transformation numérique, car plus les politiques de cybersécurité sont appliquées avec précision, plus la capacité de l'institution à prévenir et à combattre la corruption augmente, en tenant compte des intrusions externes et du développement des technologies utilisées pour détecter les vulnérabilités, ainsi que des menaces internes résultant de la complicité de certaines personnes corrompues à l'intérieur de l'institution, étant donné qu'une menace interne équivaut aux efforts des institutions essayant de pénétrer de l'extérieur ; nous devons donc constamment travailler à :

1-sensibiliser les utilisateurs à l'importance de la cybersécurité et accroître leurs capacités.

2-mettre à jour les systèmes et programmes utilisés périodiquement et en faire le suivi.

3-utiliser des programmes de sécurité pour détecter et analyser les cyberattaques. 4-suivre le développement mondial dans ce domaine, notamment en utilisant les technologies de l'intelligence artificielle.

La cybersécurité comprend trois composants de base, à savoir : «Personnes, Procédures ou Processus et Technologie «qui doivent être intégrés pour atteindre la cybersécurit car l'achat des derniers systèmes et la prise des meilleures mesures sont inutiles sans des cadres conscients capables de comprendre le système et de travailler avec lui. De même, la présence de cadres conscients et de technologies modernes avancées sans procédures et politiques claires est gaspillage d'argent, c'est donc un trio intégré dans lequel chaque composant est indispensable pour l'autre.

Afin de parvenir à une gouvernance de la cybersécurité au sein des institutions étatiques et autres, une stratégie de cybersécurité devrait être adoptée qui inclut l'élaboration de cadres législatifs et réglementaires stricts et des politiques annoncées réglementant les procédures, les pratiques et la responsabilité au sein des systèmes numériques. Les responsabilités et les pouvoirs doivent être clairement définis entre les entités chargées de la mise en œuvre et de l'audit pour éviter toute interférence, et il devrait y avoir des mécanismes spécifiques et clairs de contrôle et de responsabilité à l'égard des secteurs public et privé.

En effet, la relation entre la cybersécurité et la Lutte contre la Corruption est toujours directe, plus il y a de sensibilisation et d'intérêt pour l'application des normes et des contrôles de cybersécurité, plus il y a de prévention et de lutte contre la corruption en permettant la cyber gouvernance, qui est le nerf de la cybersécurité. Et chaque fois que des pays et des institutions se tournent vers elle, les résultats sont impressionnants, car la présence d'une cyberpolitique claire, serrée et annoncée augmente la transparence et permet un suivi, tantôt en classant les données et les informations, en déterminant les pouvoirs des utilisateurs pour y accéder et la possibilité de les modifier, et tantôt en analysant les résultats des systèmes automatisés. Après que le terme «procédures de réingénierie et de contrôle» était dominant avant la transformation numérique et l'existence de procédures et d'instructions spécifiques pour responsabiliser l'auteur et le défaillant, le critère optimal d'audit et d'examen, avec la transformation numérique, devient la présence de politiques et de

L'une des formes les plus dangereuses de cybercriminalité est celle qui cible les secteurs gouvernementaux, en particulier ceux chargés de lutter contre la Corruption. Ces secteurs ont besoin d'une protection élevée de leurs données et systèmes contre toute interférence externe visant à affecter leur processus de travail, à divulguer des informations confidentielles, à modifier les résultats des enquêtes, à les discréditer ou à perturber leurs services.

L'Égypte s'est très tôt intéressée au domaine de la cybersécurité et a cherché à diriger la scène arabe et africaine dans les indicateurs internationaux , et était également à l›avant-garde des pays visant une amélioration continue et créant une expérience réussie et pionnière au Moyen-Orient. Par conséquent, l'Egypte a atteint la neuvième place au niveau mondial dans l'indice mondial de la cybersécurité «GCI» pour 2014, et sous la gouvernance de la cybersécurité au niveau national, l'Égypte a publié la stratégie nationale pour la cybersécurité 2017-2021 conformément aux tendances mondiales modernes et aux droits contenus dans la Constitution

contrôles de cybersécurité, ainsi l'importance de la cybersécurité et son rôle efficace dans la prévention et la lutte contre la corruption deviennent clairs. Et puisque la lutte contre la corruption est l'un des défis les plus importants auxquels sont confrontées les sociétés du monde entier, et que les cybermenaces constituent une partie essentielle de ces défis, la lutte contre la corruption par la cybersécurité nécessite donc l›utilisation d›un large gamme d›outils et d›applications permettant de détecter et de prévenir les cybercrimes afin de prévenir la corruption, à savoir :

Les outils de surveillance des réseaux aident à surveiller les activités illégales sur les réseaux et à limiter les cyberrisques et les cyberattaques, de préférence via le « Network Operations Center».

Les outils d'analyse des données sont utilisés pour identifier des schémas inhabituels ou suspects et conformément aux perceptions proportionnelles à la nature des bases de données et des fonctions.

Les Outils de cryptage et de décryptage des données utilisés pour protéger les données sensibles.

Les Outils de protection anti-virus et logiciels malveillants et travaux pour les bloquer et les supprimer.

Les Outils de gestion des identités, d'accès et de vérification pour les utilisateurs autorisés.

Les Outils de gestion des autorisations qui gèrent et attribuent des autorisations de compte.

Les Outils de gestion des incidents cybernétiques qui aident à restaurer les systèmes et les données.

Le véritable défi au stade actuel est la transition vers la transformation numérique sans la capacité de la suivre avec une couverture et une base solides pour la cybersécurité, l'incapacité à gérer les dépenses couvrant la cybersécurité est une erreur évidente qui entrave la progression du processus administratif , car le volume des dépenses en cybersécurité dans les institutions ne représente pas un pour cent du volume des pertes, en particulier dans certaines attaques de ransomware et le cryptage des données, ainsi que la fuite de données sensibles, d'autant plus qu'il s'agit des actifs numériques qui doivent être protégés de l'infrastructure de l'État, en particulier les actifs critiques, il suffit de dire que le coût des cyberattaques sur l'économie mondiale devrait dépasser la barrière de 11,5 billions de dollars américains en 2023, et le coût mondial de la cybercriminalité atteindra 23 billions de dollars américains d'ici 2027.

Nous avons de nombreux défis et risques, mais les défis de la lutte contre la corruption, notamment la cybercriminalité, représentent une nouvelle forme qui nécessite la capacité de l'affronter et de la repousser, et ce en préparant une étude analytique des systèmes et en expliquant la raison de l'octroi et de la prévention des pouvoirs, en passant par le test du code source du système et l'examen des vulnérabilités et leur traitement pour les résoudre, jusqu'aux rapports d'évaluation et indicateurs de performance pour l'ensemble du système, car la détermination des pouvoirs en fonction des qualités et des titres de poste sur le système ajuste la performance et la gouvernance des compétences. La raison principale en est que «la connaissance au besoin» - le critère du besoin à cet égard est l'attribut fonctionnel - empêche toute corruption résultant d'un chevauchement des compétences ou d'un manque de clarté ou d'exploitation des utilisateurs, car chaque détenteur de pouvoir est tenu de le maintenir et de le préserver dans la mesure où il porte la responsabilité de le violer ou de compromettre ce qui lui est attribué au sein du système électronique, et il n'y a pas de déni de responsabilité à la lumière de l'identification des identités numériques et de l'accès aux exigences de chaque utilisateur par le biais de systèmes de vérification d'identité et autres. De plus, travailler au sein des systèmes étatiques, notamment en cas de différences, de technologies et de structure, nécessite un haut niveau d'expertise et de flexibilité dans le domaine de la sécurisation, de l'analyse et du traitement des données, en tenant compte des lois et réglementations régissant, le «Big Data» est «le pétrole» de l'avenir et détecter les schémas de manipulation est la capacité d'analyser ce pétrole et d'y prévenir et combattre la corruption.