Revue Internationale du Chercheur
ISSN: 2726-5889
Volume 6 : Numéro 2

La sécurité informatique dans l'administration électronique

Information Security in Electronic Administration

ASSADI FATIMA
Docteure en droit privé
Faculté des sciences juridiques et politiques- Settat
Université HASSAN Premier
MAROC

Date de soumission : 30/04/2025
Date d'acceptation : 01/06/2025
Pour citer cet article :
ASSADI. F (2025) «La sécurité informatique dans l'administration électronique», Revue Internationale du chercheur «Volume 6 : Numéro 2» pp : 810 - 825

Résumé

Depuis l'arrivée d'Internet en 1995, la digitalisation de l'administration publique marocaine a connu une évolution continue, portée par des stratégies nationales telles que « e-Maroc 2010 » et « Maroc Digital 2020 ». L'objectif principal est de moderniser les services destinés aux citoyens, aux entreprises et aux institutions publiques.

Cependant, cette transformation numérique s'accompagne de défis majeurs en matière de cybersécurité. La protection des données publiques repose à la fois sur des mesures techniques (cryptage, pare-feu, authentification) et des dispositifs physiques. Face à l'augmentation des cybermenaces, il devient crucial d'adopter une approche proactive pour garantir la confidentialité, l'intégrité et la disponibilité des informations.

Par ailleurs, la sécurité normative, fondée sur la conformité aux lois nationales et aux standards internationaux comme les normes ISO/IEC 27000, joue un rôle essentiel dans la gouvernance des systèmes d'information. L'identification des risques, la mobilisation de ressources adaptées, la sensibilisation des acteurs publics et l'utilisation de méthodes structurées (telles que PDCA ou MEHARI) sont indispensables.

En somme, la réussite de la digitalisation au Maroc repose sur un équilibre entre innovation technologique et rigueur normative, afin de bâtir une administration numérique sécurisée, résiliente et digne de confiance.

Mots clés : digitalisation ; administration publique ; cybersécurité ; données ; gouvernance.

Abstract

Since the introduction of the Internet in 1995, the digitalization of Morocco's public administration has steadily progressed through national strategies such as "e-Maroc 2010" and "Maroc Digital 2020." The main objective is to modernize services provided to citizens, businesses, and public institutions.

However, this digital transformation brings major cybersecurity challenges. The protection of public data relies on both technical measures (encryption, firewalls, authentication) and physical safeguards. In the face of increasing cyber threats, adopting a proactive approach is essential to ensure the confidentiality, integrity, and availability of information.

In addition, normative security—based on compliance with national laws and international standards such as ISO/IEC 27000—plays a key role in the governance of information systems. Identifying risks, allocating appropriate resources, raising awareness among public stakeholders, and applying structured methods (such as PDCA or MEHARI) are all critical components.

Ultimately, the success of Morocco's digitalization efforts depends on striking a balance between technological innovation and regulatory rigor. This is necessary to build a secure, resilient, and trustworthy digital administration that respects citizens' privacy.

Keywords: digitalization ; public administration ; cybersecurity ; data ; governance.

Introduction

Aujourd'hui, l'accès aux données publiques ne se limite plus à un usage interne des administrations, mais vise à fournir des services à distance pour les administrations, les entreprises et les citoyens. Le Maroc, conscient de l'importance de la transformation numérique, a mis en place une politique de numérisation, suivant les étapes de familiarisation, d'adaptation et de sécurisation.

Historiquement, depuis l'introduction de l'Internet en 1995, le Maroc a toujours cherché à entamer la transformation numérique sans un objectif unique préalablement défini. Le Plan Quinquennal 1999-2003 a intégré le développement des télécommunications et des TIC comme une priorité nationale et une option stratégique pour le développement économique, industriel et social du Royaume. Le contrat programme 1993-1997 entre l'État et l'ONPT[1] a initié le Maroc à étendre et moderniser ses réseaux de télécommunications. En outre, dès 1995, l'initiative « Maroc Compétitif » a défini des stratégies de développement de la compétitivité et de la sécurité, marquant ainsi le début d'une réflexion approfondie. En 2001, la première version opérationnelle de la « Stratégie e-Maroc » a été présentée, suivie du lancement de la stratégie « e-Maroc 2010 ». Dans le cadre de la chronologie de la transformation numérique au Maroc, il est à noter qu'en 2003, le pays a créé le Comité National e-Gov pour développer l'administration électronique, simultanément à la promulgation de la loi 55-01 modifiant la loi 24-96 sur les télécommunications. Cette genèse de la transformation numérique a été concrétisée en 2009 avec le lancement de la stratégie nationale pour la société de l'information et l'économie numérique « Maroc Numeric 2013 », suivi du Plan Maroc Digital 2020.

Le sujet de la sécurité informatique dans l'administration électronique revêt une importance scientifique, car son étude est caractérisée par un manque de données. Avant d'explorer les diverses définitions, il est important de noter l'existence de nombreuses étiquettes utilisées pour décrire l'application des technologies de l'information dans l'activité administrative, notamment l'e-gouvernement, le gouvernement numérique, l'e-administration, ainsi que l'administration électronique, entre autres.

La pluralité de cette terminologie semble découler des conceptions propres à chaque pays. Cependant, la plupart des chercheurs préfèrent utiliser le terme « administration électronique » car il est plus spécifique et moins ambigu que le terme « gouvernement », qui est souvent

[1] Office National des Postes et Télécommunications

associé à des aspects politiques plutôt qu'administratifs. Il existe en effet un écart entre la signification constitutionnelle du gouvernement et le concept d'e-gouvernement.

Plusieurs définitions de l'administration électronique ont été avancées. Certains chercheurs considèrent comme un moyen d'améliorer la performance et l'efficacité du gouvernement sans chercher à le remplacer ou à mettre fin à son rôle, D'autres la séparation comme un concept administratif englobant un ensemble de processus organisationnels qui impliquent l'interaction électronique entre les citoyens et l'administration pour atteindre des objectifs de service public, c'est pour cette raison nous avons posé la problématique suivante :

- ***Comment le Maroc peut-il garantir une protection efficace de ses systèmes d'information tout en assurant la conformité aux normes juridiques et techniques internationales, afin de préserver la confiance des citoyens dans l'administration électronique ?***

Pour répondre à cette problématique, une méthodologie analytique basée sur une approche qualitative sera adoptée. Elle reposera sur l'analyse des lois, stratégies nationales et normes internationales, ainsi qu'une étude comparative avec d'autres pays. Cette démarche permettra d'identifier les écarts, les défis et de formuler des recommandations pour améliorer la protection des systèmes d'information et renforcer la confiance des citoyens dans l'administration électronique.

Dans le cadre de cette étude, nous aborderons dans un premier temps la sécurité informatique, en adoptant une approche holistique qui met en avant la cybersécurité comme pilier essentiel de la confiance numérique dans l'administration électronique. Nous analyserons également les enjeux de confiance spécifiques à ce contexte. Ensuite, nous nous intéresserons aux systèmes de détection et de prévention des intrusions, avant d'examiner la sécurité des systèmes Cloud utilisés par les administrations. En second lieu nous traiterons la sécurité normative, en commençant par l'évaluation des enjeux et des risques liés à la protection des systèmes d'information. Nous analyserons ensuite les ressources humaines, techniques et organisationnelles mobilisées pour faire face à ces enjeux, avant de présenter les solutions de prévention identifiées comme étant les plus pertinentes.

1. Sécurité Informatique

Au sein de la doctrine, la sécurité informatique est rigoureusement définie comme une discipline ayant pour objectif premier de sauvegarder l'intégrité et la confidentialité des

informations stockées au sein d'un système informatique. Cette protection exhaustive s'étend de manière convergente sur deux fronts cruciaux :
le niveau logique, englobant le développement de logiciels sophistiqués, et le niveau physique, déployant des dispositifs matériels sécurisés.
À un niveau logique, la sécurité informatique met l'accent sur la conception et l'implémentation de logiciels robustes, utilisant des algorithmes de cryptographie avancés, des mécanismes d'authentification solides, et des protocoles sécurisés pour prévenir toute altération ou accès non autorisé aux données. Cette approche logique vise à renforcer les barrières numériques, empêchant toute violation de la confidentialité des informations stockées dans le système.(Assadi fatima, 2024)
D'un autre côté, au niveau physique, la sécurité informatique s'articule autour de dispositifs matériels conçus pour protéger les composants essentiels du système contre des accès non autorisés. Cela peut inclure des contrôles d'accès physiques, des systèmes de surveillance, et d'autres mesures visant à restreindre l'accès aux serveurs et aux centres de données où les informations sensibles sont conservées.

1.1. Une approche holistique de la sécurité informatique : dispositifs techniques et protections synchronisées

La sécurité informatique, dans son approche complète, s'efforce d'ériger des défenses à la fois logiques et physiques pour préserver l'intégrité et la confidentialité des données au sein des systèmes informatiques. Cette démarche holistique est cruciale dans un paysage numérique en constante évolution, où les menaces sont diverses et en perpétuelle mutation. D'un point de vue technique, la sécurité informatique s'appuie sur une panoplie d'outils sophistiqués et de dispositifs spécialisés, chacun jouant un rôle déterminant dans la préservation de l'intégrité des systèmes informatiques. Parmi ces éléments essentiels, les programmes antivirus se distinguent en tant que gardiens vigilants, détectant et éliminant les menaces potentielles telles que les logiciels malveillants et les virus. Ces programmes, constamment mis à jour, forment la première ligne de défense contre les attaques visant à compromettre la sécurité des données. Les pares feux, quant à eux, érigent des barrières virtuelles pour filtrer le trafic réseau et empêcher tout accès non autorisé. Ces dispositifs scrutent en permanence les communications entrantes et sortantes, appliquant des règles de sécurité strictes pour prévenir les intrusions et les activités suspectes. Le chiffrement des données constitue une autre couche cruciale de la sécurité informatique. Il s'agit d'un processus complexe qui transforme les informations en un

format illisible pour toute personne non autorisée, sauf pour ceux qui détiennent la clé de déchiffrement appropriée. Cette technique sécurise les données sensibles, qu'elles soient en transit à travers le réseau ou stockées dans des bases de données.

Parallèlement, les mécanismes d'authentification, tels que les mots de passe, forment un élément fondamental de la sécurité technique. Ils garantissent que seules les personnes ou les systèmes autorisés peuvent accéder aux données du système. Cependant, avec l'évolution des cybermenaces, d'autres méthodes d'authentification, comme la biométrie et l'authentification à deux facteurs, gagnent en importance pour renforcer la sécurité. La sécurité informatique, dans son volet technique, repose sur une diversité d'outils et de dispositifs collaborant de manière synchronisée pour garantir que seuls les acteurs autorisés puissent interagir avec le système et accéder aux données, qu'elles revêtent un caractère sensible ou non. Cette approche multifacette constitue un rempart essentiel contre les menaces numériques en constante évolution.[2]

1.1.1 La cybersécurité comme fondement de la confiance numérique dans l'administration électronique

Avec la généralisation de l'ouverture des systèmes informatiques vers l'extérieur et leur rôle stratégique crucial, la sécurité informatique évolue pour devenir un enjeu majeur, particulièrement dans le contexte de l'administration électronique. La digitalisation croissante des services publics et la connectivité accrue entre les entités gouvernementales et les citoyens exposent les données sensibles à des risques accrus, nécessitant une approche proactive et robuste en matière de sécurité.

Le contexte contemporain est marqué par une augmentation significative des menaces, la croissance exponentielle de la cybercriminalité étant l'une des principales préoccupations. La sécurité informatique doit donc anticiper et contrer diverses attaques, telles que l'espionnage, le vol de données, le sabotage, et l'usurpation d'identité, qui peuvent compromettre l'intégrité, la confidentialité et la disponibilité des données numériques.

L'approche proactive de la sécurité informatique implique la mise en place de mécanismes de défense en amont pour prévenir ces menaces plutôt que de simplement réagir après leur survenue. Cela englobe des stratégies de détection précoce, la mise en œuvre de protocoles de sécurité avancés, et le renforcement continu des infrastructures numériques. La protection des données numériques doit être intégrée dès la conception des systèmes, avec des mesures de

[2] Dr. Nasr Hajji, L'insertion du Maroc dans la société de l'information et du savoir.

sécurité adaptatives capables de faire face aux nouvelles méthodes d'attaques.(Fabrice Mattatia, 2016)

Dans cet environnement en constante évolution, la sécurité informatique devient une composante indispensable de la confiance numérique. Les citoyens et les partenaires, qu'ils soient des individus, des entreprises ou d'autres entités gouvernementales, accordent une importance capitale à la protection de leurs informations personnelles et confidentielles. La sécurité informatique devient ainsi un pilier essentiel pour garantir la crédibilité et l'intégrité des services numériques proposés par l'administration électronique. La sécurisation des systèmes informatiques dans le contexte de l'administration électronique nécessite une approche proactive, adaptative et rigoureuse pour faire face aux multiples menaces émergentes. Elle doit évoluer en tandem avec l'avancement des technologies et les nouvelles formes de cybermenaces pour assurer une protection efficace des données dans un environnement numérique en constante mutation.

La sécurité informatique constitue un pilier incontournable de la confiance numérique, revêtant une importance cruciale tant pour les partenaires que pour les citoyens. Ces derniers, qu'ils partagent leurs données de manière volontaire lors de transactions en ligne ou qu'elles soient collectées de manière involontaire, placent leur confiance dans les systèmes numériques, en particulier au sein de l'administration.

Les informations personnelles des utilisateurs, une fois diffusées en ligne, sont exposées à des risques bien réels, allant de la cybercriminalité à la collecte de données à des fins de marketing.

1.1.2 Enjeux de confiance dans l'administration électronique

Dans cette ère où l'économie est étroitement centrée sur les technologies de l'information, les données personnelles sont devenues des actifs numériques précieux. Les citoyens fournissent leurs informations sensibles dans le cadre de leurs interactions avec les services en ligne, que ce soit pour des démarches administratives, des transactions financières ou des échanges professionnels. Cette interconnexion numérique, bien qu'elle facilite la vie quotidienne, expose également ces données à diverses menaces.

La cybersécurité est devenue un enjeu fondamental pour préserver la confidentialité, l'intégrité et la disponibilité des informations dans cet environnement numérique dynamique. Les risques de piratage, de vol d'identité, d'usurpation de données, et d'autres formes de cyberattaques sont omniprésents. L'administration électronique, en tant que gardienne de données sensibles, doit

garantir des mesures de sécurité rigoureuses pour protéger la confiance que les citoyens et les partenaires ont placée en elle.

De plus, le paysage numérique est également marqué par la collecte massive de données à des fins de marketing. Les entreprises et les annonceurs exploitent ces données pour personnaliser leurs offres, cibler leurs publicités et mieux comprendre les comportements des consommateurs. Cependant, cette pratique soulève des préoccupations croissantes en matière de vie privée et de protection des données, nécessitant une régulation efficace et des mécanismes de protection robustes. (ASSADI FATIMA, 2024)

Ainsi, dans cette économie numérique en constante évolution, la sécurité informatique émerge comme un garant essentiel de la confiance numérique. Elle ne se limite pas seulement à la protection des données contre les menaces cybernétiques, mais s'étend également à la préservation de la confiance du public dans l'utilisation des services en ligne. L'administration électronique, en renforçant sa posture de cybersécurité, joue un rôle clé dans la consolidation de cette confiance, favorisant ainsi un environnement numérique sûr et fiable pour tous les acteurs impliqués[3].

1.2. Les systèmes de détection et de prévention des intrusions (IDS/IPS)

La transformation numérique de l'administration s'accompagne d'une complexification croissante des infrastructures informatiques et d'une exposition accrue aux cyberattaques. Dans ce contexte, les systèmes de détection et de prévention des intrusions jouent un rôle central dans le dispositif de cybersécurité de l'administration électronique.

Un système de détection d'intrusion IDS[4] est un outil de surveillance qui analyse en temps réel les flux de données réseau ou les activités sur les systèmes d'information afin de détecter des comportements suspects ou malveillants. Il repose sur deux méthodes principales :

La détection par signatures (comparaison avec une base de données d'attaques connues) et la détection par anomalies (identification d'écarts anormaux par rapport à un comportement de référence). En cas de détection, l'IDS alerte les administrateurs mais n'intervient pas directement.

En complément, le système de prévention d'intrusion IPS [5] va plus loin en agissant automatiquement pour bloquer ou neutraliser la menace. Lorsqu'une activité malveillante est

[3] BENSOUSSAN Alain, « Internet : aspects juridiques », édition Hermès Lavoisier, 2ème édition,1998.
[4] Intrusion Detection System
[5] Intrusion Prevention System

détectée, l'IPS peut bloquer le trafic incriminé, isoler une machine compromise, ou appliquer des règles de sécurité pour limiter les dégâts. Ce type de dispositif est particulièrement utile dans les environnements critiques comme ceux des services publics, où la continuité des activités et la confidentialité des données sont primordiales.

Dans le cadre de l'administration électronique, l'implémentation de solutions IDS/IPS permet de surveiller les connexions aux portails gouvernementaux, de protéger les bases de données contenant des informations sensibles sur les citoyens et de prévenir les intrusions potentielles. Plusieurs solutions sont disponibles sur le marché, allant des outils open-source comme Snort ou Suricata, aux solutions commerciales plus avancées intégrant l'intelligence artificielle pour une détection comportementale améliorée.

Ces outils doivent s'intégrer dans une stratégie de sécurité globale, avec une surveillance continue, des mises à jour régulières des bases de signatures, et une coordination avec d'autres dispositifs comme les pare-feu, les antivirus ou les SIEM[6]. Leur efficacité repose aussi sur les compétences des équipes de sécurité, capables d'interpréter les alertes et de réagir rapidement.

1.3. La sécurité des systèmes cloud par les administrations

La migration progressive des services publics vers le cloud-computing transforme les modèles d'hébergement traditionnels de l'administration. Ce changement vise à offrir plus de flexibilité, de réduction des coûts et de rapidité dans le déploiement des services. Toutefois, il soulève des enjeux cruciaux en matière de sécurité des données et de souveraineté numérique.

Les risques liés à l'usage du cloud sont multiples : perte de contrôle sur les données hébergées chez des prestataires externes, dépendance aux fournisseurs (vendor lock-in), vulnérabilités des interfaces et API, ou encore risques d'accès non autorisé. L'administration doit alors mettre en place des mesures rigoureuses pour sécuriser l'ensemble du cycle de vie des données. Parmi les bonnes pratiques, on retrouve :

- Le chiffrement des données au repos (stockées dans le cloud) et en transit (lors de leur circulation) à l'aide de protocoles robustes comme TLS ou AES.
- La mise en place de politiques de gestion des identités et des accès (IAM) afin de s'assurer que seuls les agents autorisés peuvent consulter ou modifier des informations.

[6] Security Information and Event Management

- L'adoption d'une approche "zero trust", où aucun utilisateur ou appareil n'est automatiquement considéré comme digne de confiance, même au sein du réseau de l'administration.
- Le recours à des plans de reprise d'activité (PRA) et des plans de continuité d'activité (PCA), essentiels pour maintenir les services publics en cas d'incident ou de panne majeure.
- La mise en œuvre de journaux d'audit et de traçabilité pour surveiller les accès, identifier les actions critiques et se prémunir contre les fuites ou manipulations frauduleuses.

Par ailleurs, les administrations doivent veiller à ce que les services cloud qu'elles utilisent soient conformes aux standards de sécurité internationaux, notamment les normes ISO/IEC 27017 (sécurité dans les environnements cloud), ISO/IEC 27018 (protection des données personnelles dans le cloud) et ISO/IEC 27001 pour la gestion de la sécurité de l'information.

Enfin, la gouvernance des services cloud suppose également une clarification contractuelle des responsabilités entre l'administration et le fournisseur de services, notamment en matière de sécurité, de sauvegarde, d'accès aux données, et de conformité aux lois nationales sur la protection des données.

Ainsi, bien que le cloud représente une avancée majeure pour la modernisation de l'administration, il ne peut être adopté sans une vigilance renforcée sur la sécurité, condition indispensable à la confiance numérique.

2. La sécurité Normative

La sécurité normative, en parallèle avec la sécurité informatique, joue un rôle crucial dans la protection des systèmes d'information. Alors que la sécurité technique se concentre sur la mise en place de mesures technologiques telles que les pares-feux et les systèmes de détection d'intrusion, la sécurité normative se focalise sur le respect des normes, réglementations et bonnes pratiques en matière de sécurité de l'information.

Au Maroc, assurer la conformité aux normes et réglementations pertinentes est essentiel pour garantir la protection des données et des informations sensibles. Cela inclut le respect des lois nationales sur la confidentialité des données ainsi que des normes internationales et des réglementations sectorielles applicables. La sécurité normative englobe également des aspects tels que la gestion des risques, la gouvernance de la sécurité de l'information et la mise en œuvre de politiques et de procédures de sécurité conformes aux standards internationaux.

En résumé, au Maroc, la sécurité normative et la sécurité technique travaillent de concert pour renforcer la protection des systèmes d'information, en assurant à la fois la robustesse

technologique et le respect des normes légales et réglementaires en vigueur. La sécurisation du système d'information repose sur plusieurs aspects cruciaux.

2.1. L'évaluation des enjeux et des risques :

La sécurité débute traditionnellement par l'identification des enjeux et l'évaluation des risques numériques. La probabilité et la gravité de ces risques dictent la mise en œuvre de mesures préventives ou protectrices. La montée en puissance des cyberattaques, une menace grandiose, exerce une influence significative sur l'état de la cybersécurité. Il est ainsi préconisé de prendre en compte et d'analyser ces menaces, notamment dans le secteur public.

Une multitude d'activités présente des dangers potentiels pour la cybersécurité, y compris les activités en ligne telles que la messagerie électronique et les réseaux sociaux, des activités liées à la gestion, comme l'externalisation des activités administratives auprès de prestataires privés, peuvent également constituer des sources de risques.

Les principales vulnérabilités en matière de cybersécurité dans le secteur public ont été identifiées par Zhao et Zhao (2010). Certaines de ces vulnérabilités sont étroitement liées aux activités en ligne, comme la navigation sur Internet, la communication par courrier électronique et l'utilisation de réseaux sans fil. Ils insistent sur l'importance de détecter ces vulnérabilités pour garantir la protection de l'administration publique.

La cybersécurité en ligne est essentielle pour protéger les réseaux informatiques de l'administration publique contre les attaques. Par conséquent, cette étude examine également les activités à risque potentiel pour la cybersécurité. L'identification et l'évaluation de ces vulnérabilités et menaces, ainsi que de leurs conséquences potentielles, sont essentielles pour sélectionner et mettre en œuvre des mesures de sécurité appropriées, dans le cadre d'une analyse de risque. Enfin, un autre facteur de risque important réside dans le manque de sensibilisation au risque au niveau des autorités supérieures.

Malgré l'amélioration générale de la sensibilisation à la sécurité à tous les niveaux administratifs, des recherches antérieures ont démontré que le manque de prise de conscience des enjeux liés à la cybersécurité, notamment au sein du personnel de direction, continue de jouer un rôle crucial dans la réduction des risques. Si ces mesures de protection ne parviennent pas à prévenir une cyberattaque, la gestion des urgences entre en jeu, ce qui représente une autre ressource cruciale. La gestion des urgences implique généralement le développement et la mise en œuvre de plans d'action visant à réduire la vulnérabilité aux menaces et à faire face à l'impact

des catastrophes, un autre aspect lié aux ressources concerne l'expérience professionnelle et l'expertise du personnel. L'expertise englobe non seulement l'éducation et l'expérience d'une personne, mais aussi la nature des connaissances qu'elle a accumulées.

2.2. Ressources

En réponse aux cyberattaques, les mesures de protection jouent un rôle crucial dans la cybersécurité et sont souvent mentionnées conjointement avec les cyberattaques, les recherches ont démontrés que « 80 % des incidents liés à la sécurité de l'information résultant de causes internes ».

En raison de cette constatation, il est impératif de prendre en considération les mesures de protection interne.

Les mesures de protection englobent un large éventail, allant des méthodes traditionnelles comme les mesures physiques[131] et la formation du personnel, aux approches plus modernes et technologiques, telles que les pares-feux et les logiciels antivirus. (ASSADI FATIMA, 2024)

2.3. L'identification des solutions de prévention

Une fois que les risques potentiels ont été identifiés, évalués et qualifiés, il est nécessaire de choisir les solutions de prévention en effectuant une comparaison entre le coût d'utilisation et le risque couvert. Par la suite, la définition des plans de sécurité des systèmes informatiques en amont et en aval découle naturellement de l'évaluation des risques. Ainsi, il est évident que la sécurité des systèmes d'information repose sur diverses méthodes de sécurité informatique, notamment :

- **La Roue de Deming PDCA136 :** Cette méthode implique la planification de la mise en œuvre d'un système de sécurité adapté aux besoins spécifiques du système d'information, en prenant en compte son contexte (Plan), la mise en place des actions, l'application des mesures nécessaires (Do), une vérification basée sur une approche d'audit (Check), et enfin la mise en œuvre d'actions correctives le cas échéant (Act) ;
- **La méthode MÉHARI[7] :** La méthode MEHARI, Méthode Harmonisée d'Analyse des Risques, est élaborée par le CLUSIF, le Club de la Sécurité de l'Information Français.

[7] La méthode MEHARI permet d'évaluer la vulnérabilité du système d'information et de préciser les actions correctrices

MEHARI est l'évolution de la méthode MARION (Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux), une méthode plus ancienne137 ;

- **La méthode ISO 27000 :** ISO 27000 est une norme britannique dédiée au système de gestion de la sécurité de l'information. Elle comporte plusieurs sous-normes couvrant diverses thématiques et secteurs. Cette norme traite à la fois de la gestion des risques et du pilotage de la fonction de sécurité informatique.

➢ **Les normes internationales relatives à la protection des données :**

La protection de la vie privée, la sécurité informatique et la cybersécurité sont désormais des éléments cruciaux pour les nations, les entreprises, les organisations, et même les individus.

C'est pourquoi l'Organisation Internationale de Normalisation s'engage à établir de manière normative les exigences techniques et managériales ainsi que les directives dans ces domaines cruciaux. Cette initiative se concrétise à travers une série de normes regroupées sous l'appellation ISO/IEC 27000.

L'une des normes les plus reconnues au sein de la famille ISO/IEC 27000, et mondialement renommée en matière de sécurité informatique, est l'ISO/IEC 27001. Cette norme concerne les systèmes de gestion de la sécurité de l'information (ISMS) et leurs exigences.

➢ **La famille des normes ISO/IEC 27000 :**

Élaborée par le comité technique ISO/CEI JTC 1/SC 27, une équipe d'experts de l'ISO spécialisé dans la sécurité de l'information, la cybersécurité et la protection de la vie privée, la famille de normes s'étend de la norme ISO/IEC 27000, qui définit le vocabulaire, à la norme ISO/IEC AWI TR 27024, actuellement en cours de développement. Cette dernière se présente sous la forme d'une liste de références pour la famille de normes ISO/CEI 27000, mettant en lumière l'utilisation de cette famille de normes et les différents types d'exigences qui y sont inclus.

Il est important de noter que les normes ISO/IEC 27025, ISO/IEC 27026 et ISO/IEC 27027 ne font pas partie de la famille des normes ISO/CEI 27000. De plus, les membres restants de cette famille de normes ISO/ CEI 27000 ne suit pas nécessairement un ordre successif.[8]

Conclusion

[8] AFNOR 2018. Sécurité de l'information – Normes ISO/IEC 27000 : Guide pratique pour mettre en œuvre un SMSI. Paris : AFNOR Éditions. Un guide pratique qui présente les principales normes de la série ISO/IEC 27000, notamment ISO/IEC 27001 et ISO/IEC 27002, et leur mise en œuvre.

La digitalisation progressive de l'administration publique au Maroc illustre une volonté affirmée de modernisation et d'optimisation des services destinés aux citoyens, aux entreprises et aux administrations elles-mêmes. Depuis l'introduction de l'Internet dans les années 1990 jusqu'à la mise en œuvre de stratégies nationales ambitieuses telles que « e-Maroc 2010 » et « Maroc Digital 2020 », le Royaume a démontré une dynamique constante en faveur de l'intégration des technologies numériques dans la gestion publique.
Cependant, cette transformation numérique n'est pas sans risques. L'ouverture des systèmes d'information à l'extérieur expose les données publiques et sensibles à des menaces croissantes telles que la cybercriminalité, l'espionnage électronique, le vol de données et les atteintes à la vie privée. Face à ces défis, la question de la sécurité informatique se pose avec acuité.

La sécurité des systèmes d'information, entendue tant sous son volet technique que sous son volet normatif, est devenue un impératif stratégique. Il ne suffit plus de déployer des dispositifs techniques tels que les pare-feux, les antivirus, les mécanismes d'authentification et les protocoles de chiffrement ; il est également essentiel de garantir une conformité stricte aux normes juridiques nationales et internationales, notamment à travers les référentiels ISO/IEC 27000. Cette double exigence technique et normative vise à assurer l'intégrité, la confidentialité, et la disponibilité des données publiques tout en consolidant la confiance des usagers dans les services numériques de l'État.
En outre, la sécurisation de l'administration électronique repose sur une approche globale intégrant l'évaluation permanente des risques, l'adoption de méthodes rigoureuses de gouvernance de la sécurité (comme le PDCA ou la méthode MEHARI), et la sensibilisation continue de l'ensemble des acteurs publics aux enjeux de cybersécurité. Le facteur humain, souvent maillon faible des dispositifs de sécurité, doit être pleinement pris en compte à travers des programmes de formation et de renforcement des capacités.

Dans un environnement numérique en constante évolution, où les cybermenaces se diversifient et se sophistiquent, il est crucial que la stratégie de sécurité de l'administration marocaine soit dynamique, proactive et évolutive. L'État doit anticiper les risques émergents, investir dans l'innovation en matière de cybersécurité, renforcer la coopération internationale, et mettre en place des mécanismes de réponse rapide aux incidents de sécurité.
Ainsi, la réussite de la digitalisation de l'administration publique marocaine passe inexorablement par la mise en place d'un écosystème de sécurité robuste, aligné sur les

meilleures pratiques internationales, garantissant la protection des données personnelles et institutionnelles, et consolidant la confiance indispensable entre l'administration et les citoyens dans l'ère numérique.

BIBLIOGRAPHIE

- OCDE (2018), Revue du gouvernement numérique du Maroc, Jeter les bases de la transformation numérique du secteur public au Maroc, Editions OCDE, Paris. P. 3 et 4.
- L'Economiste | Edition N°910 Le 06/12/2000
- Dr. Nasr Hajji, L'insertion du Maroc dans la société de l'information et du savoir.
- Rapport de l'OCDE (2018), Revue du gouvernement numérique du Maroc, Jeter les bases de la transformation numérique du secteur public au Maroc, Editions OCDE, Paris.

- BENSOUSSAN, L'informatique et le droit, memento-guide, Hermès 1995, p.371
- Lambrinoudakis et al, 2003; Yixin, 2011 ; Zhao & Zhao, 201019. Yixin (2011, p. 395)
- Assadi fatima- La transition numérique de L'administration au Maroc et le droit de la protection des données à caractère personnel. Thèse soutenue publiquement en 2024.
- Addison Wesley, An Introduction to Database Systems, 2003, pp.115-117.
- Fabrice MATTATIA, « le droit des données personnelles, n'attendez pas que la CNIL ou les pirates vous tombent dessus », EYROLLES, 2ème édition, 2016, p 11LEVY P, « Qu'est-ce que le virtuel ? », Ed, la Découverte, 1995.
- Fabrice Mattatia, RGPD ET DROIT DES DONNÉES PERSONNELLES, 3 éme édition 2018, Enfin un manuel complet sur le nouveau cadre juridique issu du RGPD et de la loi Informatique et libertés de 2018.
- BENSOUSSAN Alain, « Internet : aspects juridiques », édition Hermès Lavoisier, 2ème édition,1998.
- التقرير العام للمناظرة الوطنية الأولى حول الإصلاح الاداري " الإدارة المغربية وتحديات 2010" بتاريخ 7 و 8ماي لسنة 2002.