Revue du Contrôle de la Comptabilité et de l'Audit
ISSN: 2550-469X
Numéro 7 : Décembre 2018

Impact de la loi 09-08 sur la gouvernance des systèmes d'information des administrations publiques marocaines

Impact of the 09-08 law on the governance of information systems of Moroccan public administrations

HOUSSAIN KOUNAIDI
FSE Université Mohammed V de Rabat

YOUSSEF MAZOUZ,
FSJES Université Mohamed Premier Oujda

MOHAMED KOUNAIDI
Enseignant chercheur à la FST Tanger

Résumé

La loi 09-08 sur relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel est un défi majeur pour nombre d'administrations publiques tenues de protéger les données personnelles des citoyens Marocain. Sans préciser clairement comment protéger les données, la loi 09-08 n'est pas une norme technologique et n'encourage aucune approche technologique précise. Il invite néanmoins à s'interroger sur comment initier et gérer la mise en conformité. Pour éclairer les administrations sur le rôle de la cybersécurité dans le contexte de la loi marocaine de protection des données à caractère personnel, cette article dresse un panorama du règlement et propose un Framework pour accompagner la mise en conformité et voir l'impact de la protection des données à caractère personnel sur la gouvernance de la sécurité des systèmes d'information à travers les bonnes pratiques regroupé dans la directive nationale de la sécurité des systèmes d'information (DNSSI). Ce document se penche notamment sur la notion d'état de l'art en matière de gouvernance de la sécurité des systèmes d'information et de ses avantages pour les organisations souhaitant associer les différentes briques nécessaires à la conformité. Pour aider les professionnels de l'informatique et de la conformité qui participent au projet de mise en conformité et de gestion des risques informatique, nous dévoilons la question de comment la manière de la mise en œuvre de la DNSSI peut aider les administrations publiques marocaines à atteindre la conformité à la loi 09-08, dans le but d'atteindre la gouvernance des systèmes d'information grâce à une maitrise des risques.

Mots clés : Evolutions règlementaires, Administrations publiques, gouvernance des systèmes d'information, conformité, lois législatives, sécurité, risques

Abstract

Law 09-08 on the protection of individuals with regard to the processing of personal data is a major challenge for many public administrations obliged to protect the personal data of Moroccan citizens. Without clearly specifying how to protect the data, Law 09-08 is not a technological standard and does not encourage any specific technological approach. However, it invites us to question how to initiate and manage compliance. To enlighten administrations on the role of cybersecurity in the context of the Moroccan law for the protection of personal data, this article provides an overview of the regulation and proposes a framework to accompany compliance and see the impact of protection. personal data on the governance of information systems security through best practices grouped together in the National Directive on the Security of Information Systems (DNSSI). In particular, this paper examines the state-of-the-art concept of information system security governance and its benefits for organizations wishing to combine the different bricks needed for compliance. To help the IT and compliance professionals involved in the IT compliance and risk management project, we unveil the question of how the implementation of DNSSI can help Moroccan public administrations to Achieve compliance with Law 09-08, with the aim of achieving the governance of information systems through risk control.

Keywords: Regulatory Developments, Public Administration, Information Systems Governance, Compliance, Legislative Acts, Security, Risks

Introduction

Le développement et la diffusion des technologies de l'information, en particulier Internet, créent une tendance mondiale à utiliser ces TIC et Internet pour fournir des services publics. Cette nouvelle forme d'administration électronique offre potentiellement de grands avantages à la société en ce qu'elle peut améliorer l'efficacité, la qualité et la rentabilité des services publics. Cependant, le développement des services publics en ligne comporte de nouveaux risques. Par rapport au gouvernement qui fonctionnait à l'ère péri-informatique, le gouvernement électronique implique la génération, le stockage, le traitement et le transfert de quantités beaucoup plus importantes de données à caractère personnel. Le développement et l'expansion du gouvernement électronique affectent donc le droit des individus à la vie privée, en particulier le droit à la confidentialité des informations. Il est donc nécessaire de trouver un équilibre entre les avantages sociaux promis par le gouvernement électronique et les droits individuels à la confidentialité des informations. Une protection adéquate des données à caractère personnel à travers **une gouvernance des systèmes d'information des organismes publics** est également essentielle pour renforcer la confiance du public dans l'administration en ligne et est donc essentielle au succès de l'E-gouvernement.

Les problèmes en matière de **gouvernance des Systèmes d'Information**, principalement traités dans les revues de management, ont donné lieu à la création de cadres de bonnes pratiques tels que COBIT (Moisand, 2009), (Brand, 2008) de l'ISACA ou ITIL (Moirault, 2008). Les éléments de gouvernance font aussi l'objet de publication de normes telles que la série ISO 27000 (Carpentier, 2009) qui traite de la sécurité et de la gestion des risques. Ces cadres et norme s'avèrent utiles pour orienter les décisions des managers sur les processus clés des SI.

Au Maroc la loi 09-08 constitue un cadre légal adéquat pour la protection des données à caractère personnel, il permet de doter l'arsenal juridique marocain d'un instrument juridique de protection des particuliers, contre les abus d'utilisation des données de nature à porter atteinte à leur vie privée, et d'harmoniser le système national de protection des données personnelles à celles de ses partenaires tels que définis par les instances européennes.

D'autre part, la DGSSI[1] qui relève de l'Administration de la Défense Nationale a élaboré la directive nationale de la sécurité des systèmes d'information (DNSSI), qui s'applique à tous les systèmes d'information des administrations, des organismes publics et des structures d'importance vitale, pour atteindre une gouvernance da la sécurité de leur systèmes d'information.

[1] Direction général de la sécurité des systèmes d'information

Dans cet article on va essayer de voir comment la DNSSI peut aider les établissements publics marocains à atteindre la conformité à la loi 09-08, dans le contexte de secteur public Marocain, est-ce que la conformité avec DNSSI garantit la conformité à la loi 09-08 ? Est-ce que la DNSSI peut simplifier le processus de mise en conformité à la loi 09-08. Toutefois, il y a plusieurs différences entre les deux standards. La loi 09-08 est un standard global qui fournit aux organisations publiques une vision stratégique de la manière dont elles doivent assurer la confidentialité des données. La DNSSI est un ensemble de bonnes pratiques avec un focus sur la sécurité des informations. La directive fournit des conseils pratiques sur la manière de protéger les informations et réduire les cyber-menaces.

1. Revue de littérature

1.1 La gouvernance de la sécurité des systèmes d'information

Les informations et les technologies de l'information revêtant une importance stratégique croissante, la gestion efficace des actifs informatiques et informatiques devient une préoccupation stratégique cruciale. La gouvernance informatique (ITG) traite de la gestion de l'utilisation des technologies de l'information par une entreprise. Selon l'Institut de la gouvernance informatique (2007), il «fait partie intégrante de la gouvernance d'entreprise et comprend les structures et processus de direction et d'organisation garantissant que les TI de l'organisation maintiennent et élargissent ses stratégies et ses objectifs».

La sécurité de l'information a traditionnellement été définie comme la protection de l'information et de ses éléments critiques, y compris les systèmes et le matériel qui utilisent, stockent et transmettent cette information (Whitman et Mattord, 2008). Les points de vue traditionnels sur la sécurité de l'information comprenaient l'accès aux systèmes d'information, la sécurisation des communications, la gestion de la sécurité et le développement de systèmes d'information sécurisés (Siponen et Oinas-Kukkonen, 2007). Cependant, bien que les considérations de sécurité fassent partie intégrante de la gouvernance informatique, la gouvernance de la sécurité informatique dépasse le domaine informatique. La sécurité de l'information est de plus en plus un problème économique (von Solms et von Solms, 2005) qui appelle à sa propre gouvernance (von Solms, 2006).

Dans l'environnement professionnel en réseau et toujours actif d'aujourd'hui, il peut sembler inutile d'essayer de maintenir les systèmes corrigés et protégés contre les virus, les intrusions et autres attaques. Une défense mur-à-mur reposant sur l'informatique contre toutes les éventualités imaginables est inadéquate face aux méthodes toujours nouvelles qui contournent même les pare-feu les plus robustes. Par conséquent, la sécurité de l'information doit être adaptée et

orientée par les objectifs de l'entreprise comme dans les administrations publiques et être de plus en plus liée à l'information et à son cycle de vie. Les éléments clés à protéger incluent non seulement les informations elles-mêmes, mais également des actifs organisationnels tels que la confiance, la réputation, la marque, la valeur des parties prenantes et la satisfaction du citoyen pour lesquels des violations de la sécurité pourraient avoir des effets négatifs.

La mise en œuvre et le maintien de mesures de sécurité adéquates sous toutes ces facettes doivent être considérés comme un coût non négociable des activités commerciales.

Une gouvernance efficace de la sécurité de l'information doit intégrer des considérations juridiques, managériales, opérationnelles et techniques (Allen et Westby, 2007). Il doit spécifier les rôles disposant de l'autorité, de la responsabilité et des ressources requises pour mettre en œuvre et appliquer des stratégies, des normes, des programmes de sensibilisation, des stratégies de sécurité et d'autres procédures organisationnelles. Ainsi, il établit un cadre approprié pour la prise de décision qui repose sur une prise de décision bien informée et garantit que les décisions sont adoptées, mises en œuvre et contrôlées de manière cohérente.

Un certain nombre de normes et de cadres de bonnes pratiques pour la gestion de la sécurité de l'information (ISM) ont été développés. Ces cadres aident les organisations à évaluer et à contrôler leurs risques de sécurité et à se conformer aux réglementations et exigences de gouvernance en vigueur.

Un de ces cadres est la norme internationale ISO / IEC 27002 de gestion de la sécurité de l'information, publiée par l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (CEI) et dérivée à l'origine de la norme britannique BS 7799 des stratégies de contrôle de sécurité sous 11 rubriques principales. La norme ISO / IEC 27002 souligne l'importance de la gestion des risques et recommande de ne pas appliquer toutes les directives indiquées, mais uniquement celles qui sont pertinentes. Les principes directeurs reposent sur des exigences légales ou sur les meilleures pratiques généralement acceptées et constituent les points de départ pour la mise en œuvre de la sécurité de l'information.

Une autre norme établie et complète sur la sécurité de l'information est la norme de bonne pratique pour la sécurité de l'information (SOGP), conçue par le Forum de la sécurité de l'information (ISF). La norme comprend six aspects différents, chacun étant divisé en zones de résumé et en sections détaillées. La norme complète couvre 36 zones de résumé et 166 sections.

Nous sommes d'accord avec Allen et Westby (2007) pour dire que la gouvernance et la gestion de la sécurité sont plus efficaces lorsqu'elles sont systémiques et que la responsabilité de la sécurité d'entreprise est attribuée à des rôles disposant de l'autorité, de la responsabilité et des

ressources requises pour la mettre en œuvre et la faire respecter. Nous adhérons également à la notion de Hoogervorst (2009) selon laquelle le changement doit être abordé du point de vue de la construction, qui implique des principes de conception cohérents et cohérents et intègre de manière globale divers aspects des activités et de l'organisation.

Alors que les infrastructures ISM existantes identifient différents domaines de sécurité des informations et définissent des contrôles de sécurité détaillés, elles fournissent un aperçu limité de la manière dont la sécurité des informations est systématiquement intégrée à la conception organisationnelle. Les frameworks ne contiennent généralement pas la notion de niveaux organisationnels et de dimensions horizontales pertinentes pour les rôles, les responsabilités et les règles, ainsi que les «points de connexion organisationnels horizontaux et verticaux» (Allen et Westby, 2007) nécessaires pour une sécurité efficace de l'entreprise. Essentiellement, les cadres sont représentatifs des modèles de gestion plutôt que des modèles de gouvernance.

Von Solms (2006; 2009) constituent une exception bienvenue à cette observation. Leur modèle de gouvernance de la sécurité de l'information identifie trois niveaux de gestion - stratégique, tactique et opérationnel - et trois «actions» distinctes à travers ces niveaux - diriger, exécuter et contrôler. Les «directives» de niveau stratégique sont étendues à des ensembles de politiques de sécurité de l'information, de normes et de procédures d'entreprise au niveau tactique, ainsi qu'aux directives et procédures administratives au niveau opérationnel. L'exécution a ensuite lieu au niveau le plus bas, produisant des données de mesure extraites au niveau opérationnel, compilées et intégrées au niveau tactique, puis agrégées et abstraites pour effectuer une mesure par rapport aux exigences des directives au niveau stratégique.

En raison de ce cycle de contrôle direct, le modèle représente un modèle de gouvernance, pas simplement un modèle de gestion (von Solms et von Solms, 2006).

La loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel

Inspirée de la célèbre loi française Informatique et Libertés, la loi n° 09-08 relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel a été publiée au Bulletin Officiel n° 5744 du 18 Juin 2009, après avoir été promulguée par le Décret n° 2-09-165, en date du 21 mai 2009. Elle introduit, pour la première fois, dans le paysage juridique marocain, un ensemble de dispositions légales harmonisées avec le droit européen et, notamment, avec la Directive Communautaire n° 95/46.

La loi prévoit, des clauses relatives aux objectifs, champ d'application et au référentiel du concept de protection des données personnelles, des dispositions portant sur les conditions du traitement de cette catégorie de données, les droits de la personne concernée et obligations du responsable du traitement, et la création d'une commission de contrôle de la protection de cette catégorie de données.

Les nouvelles technologies de l'information et de la communication sont en plein essor dans notre société et imposent au droit de suivre l'évolution en élaborant un cadre juridique adéquat afin de faire face aux nouvelles problématiques juridiques. Le législateur marocain a dans ce contexte adopté la loi relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel : la loi 09-08.

L'esprit du texte se lit dès le premier article qui dispose « L'informatique est au service du citoyen et évolue dans le cadre de la coopération internationale. Elle ne doit pas porter atteinte à l'identité, aux droits et aux libertés collectives ou individuelles de l'Homme. Elle ne doit pas constituer un moyen de divulguer des secrets de la vie privée des citoyens ».

Ainsi, l'objectif de la loi 09-08 est de doter l'arsenal juridique marocain d'un instrument juridique de protection des particuliers, contre les abus d'utilisation des données de nature à porter atteinte à leur vie privée, et d'harmoniser le système national de protection des données personnelles à celles de ses partenaires tels que définis par les instances européennes.

Un décret pour l'application de cette loi a été publié au Bulletin Officiel du 18 juin 2009. Une commission nationale du contrôle et de la protection des données personnels (CNDP) a été créée afin de veiller au respect et à l'exécution des dispositions de la loi précitée.

Le champ d'application de la loi doit être explicitement clarifié, avant de définir les notions clés et de déterminer les droits des citoyens et les obligations des responsables de traitement. L'apport majeur de la présente loi est la constitution de la CNDP, garant du respect des dispositions mais dont le fonctionnement et le mode de saisine demeure mystérieux.

1.2 Les données à caractère personnel

La loi 09-08 définit les données à caractère personnel comme étant toute information, de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image, concernant une personne physique identifiée ou identifiable dénommée par la loi « personne concernée ». Elle s'applique aux données à caractère personnel, automatisé en tout ou en partie mais également aux données traitées permettant d'identifier une personne dans des fichiers manuels.

Une personne est identifiable par son nom, son prénom, son adresse, son numéro de Carte Nationale, sa photographie, son courriel, son empreinte digitale, son relevé d'identité bancaire,

en somme par toute information qui constitue une donnée à caractère personnel. Le traitement de ses données peut constituer un danger pour les citoyens lorsque leurs données personnelles sont divulguées à une tierce personne, et afin de protéger les citoyens la loi 09-08 est entrée en vigueur et a mis en place un cadre juridique réglementant la matière.

Est considéré comme étant un traitement à caractère personnel toute opération ou ensemble d'opération automatisées ou non servant à la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction des données à caractère personnel.

Est considéré comme un responsable du traitement non seulement les personnes physiques ou morales marocaines dont le responsable exerce une activité sur le territoire marocain, mais s'étend également aux entreprises étrangères qui entretiennent des relations d'affaires avec leurs homologues marocaines ou qui échangent des données avec leurs filiales ou leurs maisons mères marocaines, tout en utilisant des moyens situés sur le territoire marocain.

Il s'agit ainsi de créer des conditions favorables au développement de l'offshoring et des délocalisations.

1.3 Les droits des personnes concernées

1.3.1 Le consentement indubitable de la personne concernée

Tel que prévu par l'article 4 de la loi 09-08, la communication des données à caractère personnel à un tiers nécessite indubitablement le consentement préalable de la personne concernée. L'article premier de la loi définit le consentement de la personne concernée comme étant toute manifestation de la volonté, libre, spécifique et informée, par laquelle la personne concernée accepte que les données à caractère personnel la concernant fassent l'objet d'un traitement. Cela dit la loi a émis une réserve quant à cette obligation en permettant aux responsables de divulguer certaines données, lorsque le traitement est nécessaire au respect d'une obligation légale à laquelle est soumise la personne concernée ou le responsable du traitement, ou encore lorsqu'il s'agit de l'exécution d'un contrat auquel la personne concernée est partie. Cette réserve s'étend également à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées. Abstraction faite de ses situations, les responsables du traitement sont tenus d'attendre que la personne concernée ait consentie à la communication de ses données

personnelles, à moins que cette dernière soit dans l'impossibilité physique ou juridique, d'exprimer son consentement.

La loi reconnaît également aux personnes concernées certains droits, à savoir : le droit à l'information lors de la collecte des données, le droit d'accès, le droit de rectification, le droit d'opposition.

1.3.2 Le droit à l'information lors de la collecte des données

Le droit d'information est au cœur de la protection des données car il constitue une garantie de collecte transparente et loyale des données à caractère personnel.

L'obligation d'information lors de la collecte des données prévue par l'article 5 de la loi 09-08, concerne l'information préalable de toute personne de manière précise, expresse et non équivoque de l'utilisation ou du stockage de données informatisées la concernant. Cette même personne doit également être informée sur l'organisme qui effectue la collecte d'information mais aussi sur les destinataires ou les catégories de destinataires. D'autant plus, lorsque la personne concernée répond à des questionnaires, il doit être porté à sa connaissance si la réponse à telle ou telle question est obligatoire ou facultative.

Toutefois, il existe des limites au droit d'information et notamment lorsque les informations sont traitées à des fins de statistiques, historiques ou scientifiques, dans ce cas le responsable de traitement doit en informer la commission et lui présenter les motifs de l'impossibilité d'information.

Par ailleurs, le droit de l'information n'est pas applicable aux données dont la collecte est essentielle à la défense nationale, la sûreté intérieure ou extérieure de l'Etat, à la prévention ou répression du crime.

L'exclusion est également valable lorsque la législation prévoit expressément l'enregistrement ou la communication des données à caractère personnel et lorsque le traitement est destiné à des fins exclusivement journalistiques, artistiques ou littéraires.

1.4 Les obligations des responsables de traitement

L'obligation primaire des responsables de traitement est de ne collecter des données à caractère personnel que pour des finalités déterminées, dont la personne concernée est explicitement informée. Ce dernier s'oblige à ne pas les traiter par la suite de manière incompatible avec ces finalités. En plus de cela la loi 09-08 impose une autorisation préalable de la personne concernée dans certains cas, et d'une déclaration préalable dans d'autres cas, et ce selon la nature des informations collectées.

L'article 3 de la loi 09-08 dispose que les données à caractère personnel doivent être traitées loyalement et licitement. Elles ne peuvent être collectées que pour des finalités bien déterminées et ne peuvent être conservées que pendant la durée de la réalisation des finalités pour lesquelles elles ont été collectées. Ce même article impose au responsable du traitement de ces données un devoir d'exactitude et de mise à jour, à défaut les données inexactes ou incomplètes doivent être rectifiées ou effacées.

1.4.1 Le Consentement

Toutefois, le consentement préalable n'est pas exigé si le traitement est nécessaire au respect d'une obligation légale à laquelle est soumise la personne concerné ou le responsable du traitement, à l'exécution du contrat auquel la personne est partie, à la sauvegarde d'intérêts vitaux de la personne concernée, à l'exécution d'une mission d'intérêt public ou relevant de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées, et à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire sous réserve de ne pas méconnaître l'intérêt ou les droits fondamentaux de la personne concernée.

1.4.2 L'autorisation préalable

En vertu des dispositions de l'article 12 de la loi 09-08, les responsables du traitement sont soumis à une autorisation préalable de la personne concernée lorsque les traitements concernent les données sensibles visées à l'alinéa 3 de l'article premier. La loi entend par « données sensibles », « les données à caractère personnel qui révèlent l'origine racial ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que les données relatives à la santé de la personne concernée ».

Ils sont également soumis à la dite autorisation lorsqu'il s'agit de données portant sur les infractions, condamnations ou mesures de sûreté, des données comportant le numéro de la carte d'identité nationale de la personne concernée.

Le traitement de ces données nécessite une autorisation préalable de la personne concernée lorsqu'elles sont utilisées pour d'autres finalités que celles pour lesquelles elles ont été collectées.

L'article 22 de la loi 09-08 impose aux responsables du traitement une déclaration à la Commission Nationale lorsqu'il s'agit d'un traitement de données relatives à la santé lorsqu'il est effectué par un praticien de la santé tenu du secret professionnel ou par toute autre personne soumise également à une obligation de secret.

Le défaut de l'autorisation et de la déclaration préalable est sanctionné par l'article 52 de la loi.

1.4.3 La déclaration préalable

Les responsables de traitement sont tenus en vertu des dispositions de l'article 13 de la loi 09-08 de déposer leur engagement relatif au traitement des données conformément aux prescriptions de la présente loi auprès de la Commission Nationale.

Cette obligation doit être exécutée préalablement à la mise en œuvre d'un traitement entièrement ou partiellement automatisé ou d'un ensemble de tels traitements ayant une même finalité ou des finalités liées.

La déclaration préalable doit comporter les éléments suivants :

– le nom et adresse du responsable du traitement, et le cas échéant, de son représentant

– la dénomination, les caractéristiques et la ou les finalités du traitement envisagé

– une description de la ou des catégories de personnes concernées et des données ou des catégories de données à caractère personnel s'y rapportant

– les destinataires, ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées

– les transferts de données envisagés à destination d'Etats étrangers

– la durée de conservation des données

– le service auprès duquel la personne concernée pourra exercer le cas échéant, les droits qui lui sont reconnus par les dispositions de la présente loi, ainsi que les mesures prises pour faciliter l'exercice de ceux-ci

– une description générale permettant d'apprécier de façon préliminaire le caractère approprié des mesures prises pour assurer la confidentialité et la sécurité du traitement en application des dispositions des articles 23 et 24.

– les recoupements, les interconnexions, ou toutes autres formes de rapprochement des données ainsi que leur cession, sous-traitance, sous toute forme, à des tiers à titre gratuit ou onéreux.

Il est indiqué que toute modification ou suppression de l'un quelconque des éléments susvisés doit être communiquée, sans délai, à la connaissance de la Commission.

Dans le cas de cession d'un fichier de données, le cessionnaire doit remplir les formalités de déclaration prévues par la présente loi.

Les modalités de la déclaration sont fixées par voie réglementaire.

1.4.4 Les obligations de confidentialité et de sécurité des traitements et de secret professionnel

En vertu des dispositions de l'article 23 de la loi 09-08, le responsable du traitement est tenu de mettre en œuvre toutes les mesures techniques et organisationnelles pour protéger les données à caractère personnel, afin d'empêcher qu'elles soient endommagées, modifiées, ou utilisées par un tiers non autorisé à y accéder, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute forme de traitement illicite.

D'autant plus, ce même article prévoit pour le responsable de traitement qui effectue des traitements pour son compte de choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer tout en veillant au respect de ces mesures.

1.5 La Commission nationale de contrôle de la protection des données à caractère personnel

Suite à la promulgation de La loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, une Commission Nationale de contrôle de la Protection des Données à caractère personnel a été créé le 30 août 2010.

1.5.1 Composition de la CNDP :

Instituée auprès du premier ministre, elle est chargée de mettre en œuvre et de veiller au respect des dispositions de la loi 09-08 et des textes pris pour son application. Elle se compose de 7 membres dont un président nommé par le Roi. Les six autres membres sont également nommés par le Roi, dont deux sur proposition du premier ministre, deux sur proposition du président de la Chambre des représentants, et deux sur proposition du président de la Chambre des conseillers. La durée du mandant des membres de la CNDP est de cinq ans, renouvelable une seule fois. Les membres de la Commission sont choisis parmi des personnalités du secteur public ou privé, qualifiés pour leur compétence dans le domaine juridique et judiciaire, des personnalités justifiant d'une grande expertise en matière informatique, ainsi que des personnalités reconnues pour leur connaissance des questions touchant aux libertés individuelles. La Commission est composée de cinq départements.

1.5.2 Pouvoirs de la CNDP :

La Commission veille à ce que l'informatique ne porte pas atteinte à l'identité, aux droits et aux libertés collectives ou individuelles de l'Homme et au respect des secrets de la vie privée des citoyens. Elle exerce ses missions conformément à la loi 09-08 et au décret pris pour l'application de cette loi publié au Bulletin Officiel du 18 juin 2009.

Elle est dotée de plusieurs pouvoirs qui lui ont été confié par la loi. Elle exerce un pouvoir de contrôle, de sanction, de conseil, de sensibilisation.

- La veille au respect des droits des personnes concernées :

La commission veille au respect des droits de toute personne concernée par le traitement automatique ou non des données à caractère personnel, à savoir le droit d'information, d'accès, de rectification et d'opposition. Ainsi lorsque le droit de rectification n'est pas respecté par le responsable du traitement, la Commission ordonne au responsable du traitement de procéder aux rectifications nécessaires dans un délai qui ne peut excéder sept jours à compter de la date d'envoi de la décision rendue par la Commission.

Elle contrôle les paramètres institués par les responsables des traitements pour répondre à l'obligation de confidentialité et de sécurité. A cet égard, elle contrôle le transfert des données personnelles vers un pays étranger.

- La saisine de la Commission :

La Commission peut être saisie par toute personne physique dont les données à caractère personnel font l'objet d'un traitement à travers le dépôt d'une plainte, lorsque cette dernière se sent lésée par la publication d'un traitement. Est considérée comme plainte toute dénonciation d'agissements contraire à la loi 09-08 et à ses textes d'application. La plainte peut être adressée par voie postale ou par voie électronique, ou déposée au secrétariat général. Elle doit indiquer le nom, l'adresse et la signature de son autre, et toutes indications à même de permettre d'identifier l'entité contre laquelle elle est déposée, ainsi que tous les éléments concernant les faits reprochés. La plainte est enregistrée. Un reçu portant le numéro d'enregistrement, en est délivré. Les plaintes sont examinées par le service en charge, et dans la mesure où elles relèvent de la compétence de la Commission, elles sont notifiées contre accusé de réception à l'entité à l'encontre de laquelle elles ont été faite, en vue de formuler dans un délai de 15 jours, toute observation qu'elle jugera utile. C'est ce qui ressort de l'article 37 du règlement intérieur de la Commission. La Commission est compétente pour instruire les plaintes et leur donner suite en ordonnant la publication de rectificatifs. Cette mission est confiée au département juridique de la Commission. A cet effet, elle est en mesure d'ordonner que lui soient communiqués, dans les délais et selon les modalités ou sanctions éventuelles qu'elle fixe, les documents de toute nature ou sur tous supports lui permettant d'examiner les faits concernant les plaintes dont elle est saisie. La commission peut également jouer un rôle de concertation entre les parties. Elle peut faire procéder à une mission de contrôle ou de vérification sur place, et lorsque le traitement porte atteinte à la sûreté ou à l'ordre public ou est contraire à la morale ou aux bonnes mœurs,

elle se voit dans l'obligation de retirer le récépissé de la déclaration ou de l'autorisation. Lorsqu'elle estime l'intervention de la justice nécessaire, la Commission peut saisir le procureur du Roi aux fins de poursuites. Bien entendu, le plaignant est tenu informé des suites données à sa plainte.

Lorsque la Commission décide de donner une suite judiciaire à la plainte, elle doit saisir le procureur du Roi territorialement compétent.

La Commission a également la possibilité de s'autosaisir en cas de violation des dispositions de la loi 09-08. Elle exerce à cet effet un pouvoir d'investigation et d'enquête permettant à ses agents, régulièrement commissionnés à cet effet par le président, d'avoir accès aux données faisant l'objet de traitement, de requérir l'accès direct aux locaux au sein desquels le traitement est effectué, de recueillir et de saisir toutes les informations et tous les documents nécessaire pour remplir les fonctions de contrôle, le tout conformément à la commission à laquelle ils exécutent (article 30 de la loi 09-08). Le but du contrôle sur place est de vérifier la régularité du traitement avec les dispositions de la loi n°09-08, des textes pris pour son application et du règlement intérieur de la Commission.

- Les enquêtes et investigations :

Des agents chargés du contrôle sont désignés pour effectuer les enquêtes et investigations sur place, après avoir justifié de leur commissionnement auprès de l'organisme chargé du traitement qui va subir ce contrôle. Est rédigé à la suite de chaque enquête, un procès-verbal qui doit être signé par les agents chargés du contrôle, ainsi que par le représentant du responsable du traitement, ou par toute personne chargée des opérations par le représentant. Ce procès doit comprendre la nature, le jour, l'heure et le lieu des opérations de contrôle effectuées, l'objet du contrôle, les membres de la commission ayant participé au contrôle, les personnes rencontrées et le cas échéant leurs déclarations, les demandes exprimées par les agents chargés du contrôle ainsi que les éventuelles difficultés rencontrées. C'est ce qui ressort de l'article 43 du règlement intérieur de la Commission.

Cela dit la Commission est tenu d'informer le procureur du Roi territorialement compétent de l'opération de contrôle qui sera effectuée au moins vingt-quatre heures auparavant.

A cet effet, l'article 62 de ladite loi, prévoit un emprisonnement de trois à six mois et/ou une amende allant de 10.000 à 50.000 DH à l'encontre de quiconque qui entrave l'exercice des missions de contrôle de la Commission nationale, ou qui refuse de recevoir les contrôleurs et de les laisser remplir leurs commissions, ou qui refuse d'envoyer les documents ou informations demandé(e)s, ou refuse de transmettre les documents prévus par la loi.

- Le pouvoir de sanction :

La Commission est également investie d'un pouvoir de sanction, qui lui a été confié par la loi 09-08. Dans une déclaration du président de la commission à un quotidien national, ce dernier s'exprime sur les violations avérées par les organismes détenant les données, et parle de la possibilité de la Commission d'adopter des mesures disciplinaires à leur encontre. Cela dit la procédure disciplinaire doit garantir le droit de la défense en respectant le principe du contradictoire. En effet le législateur a prévu un certain nombre de sanction pour accompagner les dispositions de la loi précitée. Ainsi toute personne qui commet une des infractions prévues par le chapitre VII de la loi, voit sa responsabilité pénale engagée, et se voit exposée à des sanctions dissuasives allant de la simple amende à l'emprisonnement, et ce en fonction de la gravité de l'infraction. Ces sanctions peuvent aller jusqu'à 300.000 DH et jusqu'à cinq ans d'emprisonnement.

- L'émission des avis :

La Commission peut émettre des avis au gouvernement ou au parlement sur les projets ou propositions de lois ou projets de règlements relatifs au traitement de données à caractère personnel dont elle est saisie, à l'autorité compétente sur les projets de règlements créant des fichiers relatifs aux données à caractère personnel recueillies et traitées à des fins de prévention et de répression des crimes et délits, sur les projets et propositions de lois portant création et traitement des données relatives aux enquêtes et données statistiques recueillies et traitées par des autorités publiques, au gouvernement sur les modalités de la déclaration, sur les modalités d'inscription au registre national institué par l'article 45 de la loi 09-08, sur les règles de procédure et de protection des données des traitements de fichiers sécurité qui doivent faire l'objet d'un enregistrement (article 27 de la loi 09-08).

- La sensibilisation :

La commission entreprend des actions de sensibilisations à destination du public, des opérateurs économiques et à l'ensemble des responsables du traitement des données à caractère personnel. A cet effet, après une réunion avec les trois opérateurs téléphoniques, ces derniers se sont engagés à limiter le harcèlement dont ils ont fait preuve via les SMS. Dans ce cadre, la commission s'est alliée aux opérateurs téléphoniques afin de mener une campagne de sensibilisation destinée aux opérateurs du marketing électronique.

La DNSSI moyen de gouvernance de la sécurité des SI pour les organismes publics

La supervision de la confiance numérique a été confiée à l'administration de la défense nationale depuis 2011. La Direction générale de la sécurité des systèmes d'information (DGSSI), a défini une nouvelle stratégie basée sur les quatre leviers suivants:

- L'évaluation des risques pesant sur les systèmes d'information au sein des administrations, organismes publics et infrastructures d'importance vitale;
- La protection et la défense des systèmes d'information des administrations, organismes publics et infrastructures d'importance vitale;
- Le renforcement des fondements de la sécurité: Cadre juridique, sensibilisation, formation et recherche & développement;
- La promotion et le développement de la coopération nationale et internationale.

Dans le cadre de cette stratégie, la DGSSI a élaboré la directive nationale de la sécurité des systèmes d'information, qui s'applique à tous les systèmes d'information des administrations, des organismes publics et des structures d'importance vitale. Cette directive a été matérialisée par la publication du décret n° 2-15-712 du 22 mars 2016 relatif à la protection des systèmes d'information sensibles des infrastructures d'importance vitale.

Pour arrêter les règles de la DNSSI, la DGSSI s'est inspirée de la norme ISO/CEI27002:2009 et s'est basée sur les résultats de l'enquête menée au mois de juillet 2013 auprès d'un échantillon représentatif d'administrations et organismes publics et d'opérateurs d'importance vitale.

2. ETUDE D'IMPACT DE LA DNSSI SUR LA PROTECTION DES DONNEES PERSONNELLES

La mise en œuvre d'un système de gestion de l'information conforme à la Directive Nationale de Sécurité des Systèmes d'Information (DNSSI) constitue non seulement une pratique exemplaire en matière de sécurité de l'information, mais elle est également essentielle pour démontrer la conformité à la protection des données.

L'article 23 de la loi 09-08 oblige les organisations à:

- Mettre en œuvre les mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisé, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite. Ces mesures doivent assurer, compte tenu de l'Etat de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger ;

- Empêcher l'accès de toute personne non autorisée aux installations utilisées pour le traitement de ces données (contrôle de l'entrée dans les installations) ;
- Empêcher que les supports de données puissent être lus, copiés, modifiés ou retirés par des personnes non autorisées (contrôle des supports de données) ;
- Empêcher l'introduction non autorisée, ainsi que la prise de connaissance, la modification ou l'élimination non autorisées de données à caractère personnel introduites (contrôle de l'insertion) ;
- Empêcher que les systèmes de traitements automatisés de données puissent être utilisés par des personnes non autorisées au moyen d'installations de transmission de données (contrôle de l'utilisation) ;
- Garantir que seules les personnes autorisées puissent avoir accès aux données visées par l'autorisation (contrôle de l'accès) ;
- Garantir la vérification des entités auxquelles les données à caractère personnel peuvent être transmises par des installations de transmission de données (contrôle de la transmission) ;
- Garantir qu'il soit possible de vérifier a posteriori, dans un délai approprié en fonction de la nature du traitement à fixer dans la réglementation applicable à chaque secteur particulier, quelles données à caractère personnel sont introduites, quand elles l'ont été et pour qui (contrôle de l'introduction) ;
- Empêcher que lors de la transmission de données à caractère personnel et du transport des supports, les données puissent être lues, reproduites, modifiées ou éliminées sans autorisation (contrôle du transport) ;

En suivant la DNSSI, les organisations du secteur public Marocain seront en mesure de mettre en œuvre des mesures de sécurité adéquates et efficaces, basées sur les résultats d'une évaluation formelle des risques, pour vous conformer à la loi 09-08.

❖ **DNSSI et conformité à la loi 09-08**

Ci-après on présentera une brève description comment de la manière la mise en œuvre de la DNSSI peut aider les établissements publiques marocaines à atteindre la conformité à la loi 09-08 :

- ASSURANCES

L'utilisation de la DNSSI inspiré de la certification ISO 27001 est un moyen de fournir l'assurance nécessaire que l'organisation gère efficacement les risques liés à la sécurité de l'information.

- PAS SEULEMENT DES DONNÉES PERSONNELLES

La DNSSI suit les meilleures pratiques internationales et aidera les organisations publiques à mettre en place des processus protégeant non seulement les informations client, mais également tous les actifs informationnels, y compris les informations stockées sous forme électronique et sous forme de copie.

- CADRE DE CONTRÔLE ET DE SÉCURITÉ

La loi 09-08 stipule que les organisations doivent sélectionner les contrôles techniques et organisationnels appropriés pour atténuer les risques identifiés. La plupart des dispositions et contrôles de protection des données de la loi 09-08 sont également recommandés par la DNSSI.

- PERSONNES, PROCESSUS ET TECHNOLOGIES

La DNSSI englobe les trois aspects essentiels de la sécurité de l'information: les personnes, les processus et la technologie, ce qui signifie que l'organisation est protégée non seulement contre des risques liés à la technologie, mais également d'autres menaces plus courantes, telles qu'un personnel mal informé ou des procédures inefficaces.

- RESPONSABILITÉ

La DNSSI exige que le système de sécurité soit soutenu par les plus hauts responsables et intégré à la culture et à la stratégie de l'organisation. Cela nécessite également la nomination d'un haut responsable qui assume la responsabilité du SGSI. LA loi 09-08 exige une la nomination d'un responsable de traitement qui a une responsabilité claire en matière de protection des données dans l'ensemble de l'organisation.

- EVALUATION DES RISQUES

La conformité à la DNSSI implique de procéder à des évaluations régulières des risques afin d'identifier les menaces et les vulnérabilités pouvant affecter vos actifs informationnels, ainsi que de -prendre des mesures pour protéger ces données.

La loi 09-08 exige spécifiquement une évaluation des risques afin de s'assurer qu'une organisation a identifié les risques pouvant avoir une incidence sur les données personnelles.

- AMELIORATION CONTINUE

La DNSSI exige que votre la politique de sécurité soit surveillé, mis à jour et révisé en permanence, ce qui signifie qu'il évolue au fur et à mesure que l'organisation évolue en suivant un processus d'amélioration continue. Cela signifie que votre cette politique s'adaptera aux changements - internes et externes - à mesure que d'identifier et de réduire les risques en permanence.

Conclusion

La loi 09-08 et la DNSSI sont deux standards qui ont beaucoup en commun. Tous deux visent à renforcer la sécurité des données et réduire le risque de failles de sécurité, et tous deux exigent des administrations publiques qu'elles assurent la confidentialité, l'intégrité et la disponibilité des données sensibles. La DNSSI est inspiré de la norme ISO 27002 qui est l'un des standards de bonnes pratiques les plus détaillés en la matière, et il faut noter que les dispositions de la loi 09-08 implique une adhésion aux codes de conduite et certifications approuvées – comme la DNSSI – peut être utilisée pour démontrer la conformité.

La loi 09-08 se concentre sur la confidentialité des données et la protection des informations personnelles. Il impose aux entreprises de déployer les moyens nécessaires pour obtenir un consentement explicite pour collecter des données et s'assurer que ces données sont traitées de manière légale. Toutefois, il ne donne pas les détails techniques sur la manière de maintenir un niveau de sécurité des données adéquat ou pour réduire les menaces internes et externes. A cet égard, la DNSSI apporte des réponses : la norme fournit des orientations pratiques sur la manière de développer des politiques claires et complètes pour réduire les risques qui peuvent générer des incidents de sécurité.

Bien que la conformité à la DNSSI ne garantisse pas la conformité à la loi 09-08, elle peut être une étape qui présente un intérêt certain. Les administrations publiques ont donc intérêt à considérer la possibilité de se certifier à la DNSSI pour s'assurer que leurs mesures de sécurité sont suffisamment fortes pour protéger les données sensibles.

La loi 09-08 qui dispose d'une section relatif aux sanctions oblige les organisations à se conformer à ses dispositions, -comme on l'a montré dans notre article- la DNSSI qui aide les organisations publiques à se conformer à la dite loi, constitue un élément indispensable pour la réalisation de la gouvernance de la sécurité des systèmes d'information.

Référence :

Moisand, (2009).COBIT : Pour une meilleure gouvernance des systèmes d'information, Groupe Eyrolles, France

Brand, (2008). L'ISACA : Information System Audit and Control Association

Moirault, (2008) ITIL : Les meilleures pratiques de gestion d'un Service informatique version 3

Textes et lois :

Decret-2-09-165-Ar

Loi 09-08-Fr

Reglements-Interieurs- CNDP-Fr

Textes législatifs et réglementaires DGSSI

Rapports :

Rapport-activite-CNDP-2010-2013-fr.pdf

Webographies :

http://www.cndp.ma

https://www.dgssi.gov.ma

https://www.cnil.fr