Revue Internationale du Chercheur
ISSN: 2726-5889
Volume 4 : Numéro 3

PROTECTION DES DONNEES PERSONNELLES ET CYBERSECURITE

PROTECTION OF PERSONAL DATA AND CYBERSECURITY

Pr. AKKOUR SOUMAYA
Professeure d'enseignement supérieur
Faculté des Sciences Juridiques et Politiques
Université Hassan Premier
Laboratoire De Recherche En Dynamiques Sécuritaires.
Maroc
Soumiasta@yahoo.fr

ASSADI Fatima
Doctorante chercheuse en Droit Du Numérique et des nouvelles technologies
Faculté des sciences juridiques et politiques
Université Hassan premier
Laboratoire De Recherche En Dynamiques Sécuritaires
Maroc
fatimassadi@gmail.com

HAOUNANI Amine
Doctorant chercheur en Droit Du Numérique et des nouvelles technologies.
Faculté des sciences juridiques et politiques
Université Hassan premier
Laboratoire De Recherche En Dynamiques Sécuritaires.
Maroc
a.haounani@uhp.ac.ma

Date de soumission : 17/06/2023

Date d'acceptation : 05/08/2023

Pour citer cet article :

AKKOUR S. & al. (2023) «PROTECTION DES DONNEES PERSONNELLES ET CYBERSECURITE», Revue Internationale du Chercheur «Volume 4: Numéro 3» pp: 1 – 23

Résumé

La protection des données personnelles et la cybersécurité sont des enjeux majeurs ayant un impact considérable sur les individus et les organisations. La protection des données concerne la collecte, le stockage, l'utilisation et la divulgation des informations personnelles, tandis que la cybersécurité vise à préserver les systèmes informatiques et les données contre les attaques cybernétiques. Des lois strictes telles que le RGPD de l'UE et La loi 09-08 relative à la protection des données à caractère personnel au Maroc garantissent la protection des données personnelles et imposent des obligations aux entreprises. Les organisations doivent mettre en place des mesures de cybersécurité, tandis que les consommateurs peuvent aussi protéger leurs informations. La vigilance et l'adoption de pratiques de sécurité évoluées sont essentielles. La collaboration entre gouvernements et entreprises est cruciale pour garantir la protection des données personnelles et la cybersécurité.

En somme, cet article souligne l'importance de ces domaines et promeut la nécessité d'une coopération étroite entre gouvernements, entreprises et consommateurs pour assurer leur protection.

Mots clés : Données personnelles ; cyberespace ; vie privée ; sécurité ; CNDP.

Abstract:

The protection of personal data and cybersecurity are major issues with a significant impact on individuals and organizations. Data protection involves the collection, storage, use, and disclosure of personal information, while cybersecurity aims to safeguard computer systems and data against cyber-attacks. Strict laws such as the EU's GDPR and Morocco's Law 09-08 on the protection of personal data ensure the protection of personal data and impose obligations on businesses. Organizations need to implement cybersecurity measures, and consumers can also protect their information. Vigilance and the adoption of advanced security practices are essential. Collaboration between governments and businesses is crucial to ensuring the protection of personal data and cybersecurity. In summary, this article highlights the importance of these areas and promotes the need for close cooperation between governments, businesses, and consumers to ensure their protection.

Keywords: Personal data ; cyberspace ; privacy ; security ; CNDP.

Introduction:

Le monde numérique a considérablement transformé la manière dont les informations personnelles sont collectées, stockées et utilisées. Les entreprises, les gouvernements et d'autres organisations collectent et utilisent des quantités massives de données personnelles pour améliorer les produits et services, fournir une publicité ciblée et mieux comprendre les consommateurs. Cependant, cette collecte de données soulève des préoccupations en matière de vie privée et de protection des données. Les lois sur la protection des données personnelles telles que le Règlement Général de la Protection des Données personnelles en Europe et la loi 09-08 relative à la protection des données à caractère personnel au Maroc sont en place pour garantir que les informations personnelles sont protégées et utilisées de manière responsable. Les consommateurs peuvent également prendre des mesures pour protéger leurs informations en ligne, telles que la vérification de la sécurité des sites web et la restriction de l'information partagée en ligne. Il est important de continuer à surveiller les développements dans ce domaine pour protéger les informations personnelles dans le monde numérique.

Les données personnelles peuvent être définies comme toute information concernant une personne physique identifiée ou identifiable. Cela peut inclure des informations telles que le nom, l'adresse, les informations de contact, les informations financières et les données biométriques. La protection des données personnelles implique la gestion sécurisée de ces informations pour garantir la vie privée et la sécurité des individus. [LEPAGE A., Libertés et droits fondamentaux à l'épreuve de l'Internet : droits de l'internaute, liberté d'expression sur l'Internet, responsabilité, Litec, 2002]. La cybersécurité, quant à elle, se concentre sur la protection des systèmes informatiques, des réseaux et des données en ligne contre les menaces et les attaques. Cela inclut des mesures telles que la mise en place de pare-feu, la détection et la prévention des intrusions, la sécurisation des données et la formation aux bonnes pratiques en matière de sécurité. La relation entre les données personnelles et la cybersécurité est étroitement liée, les informations personnelles sont souvent stockées et traitées en ligne, ce qui les expose à des risques de sécurité tels que les cyberattaques. Par conséquent, la protection des données personnelles implique souvent la mise en œuvre de mesures de cybersécurité pour garantir la sécurité des informations en question. Les deux concepts sont donc étroitement liés pour garantir la protection des informations personnelles et la sécurité des systèmes informatiques.

Les données personnelles et la cybersécurité sont d'une importance critique pour les individus et les organisations. La protection des données personnelles garantit la confidentialité et la

sécurité des informations personnelles des individus, telles que leurs noms, adresses, numéros de téléphone, informations financières, etc. Cela contribue à la protection de la vie privée et à la prévention de l'utilisation abusive des informations personnelles. De même, la cybersécurité est cruciale pour la protection des systèmes informatiques et des données en ligne contre les cyberattaques telles que les violations de données, les rançongiciels et le phishing. Pour les organisations, la sécurité des données et des systèmes informatiques est cruciale pour préserver leur réputation, leur crédibilité et leur rentabilité. Les cyberattaques peuvent également entraîner des coûts importants pour les organisations en matière de récupération de données et de remise en état des systèmes informatiques. [Bank Aurélie RGPD 2019].

Pour les individus, la cybersécurité est importante pour protéger leurs informations personnelles et financières en ligne et pour éviter les pertes financières. Les données personnelles peuvent également être utilisées pour le marketing ciblé, les études de marché et la surveillance en ligne, ce qui peut porter atteinte à la vie privée des individus.

❖ La question qui se pose est de savoir si la législation marocaine sur la protection des données à caractère personnel est efficace pour assurer la protection des données personnelles ? et quelles sont les mesures que les consommateurs peuvent prendre pour protéger leurs données personnelles dans le cyberespace ?

Nous adopterons une approche méthodologique analytique pour aborder cette problématique. Dans cette optique, nous examinerons d'abord l'arsenal juridique et institutionnel en vigueur au Maroc concernant les données personnelles et le cyberespace **(1)**. Ensuite, nous nous intéresserons aux mesures préventives visant à renforcer la protection dans le cyberespace **(2)**.Cette méthodologie nous permettra d'analyser en détail les différentes lois, réglementations et institutions impliquées dans la protection des données personnelles et du cyberespace au Maroc.

1. Le cadre juridique et institutionnel des données personnelles et de la cybersécurité au Maroc

Dans l'ère numérique d'aujourd'hui, la protection des données personnelles et la cybersécurité sont devenues des enjeux majeurs. Le Maroc a su répondre à ces défis en mettant en place un cadre juridique et institutionnel solide pour garantir la confidentialité, l'intégrité et la sécurité des données personnelles, ainsi que pour assurer la protection contre les cybermenaces.

Dans cet partie, nous explorerons le cadre juridique du cyberespace au Maroc, en mettant l'accent sur les lois, les réglementations et les politiques qui régissent la protection des données

personnelles, la cybersécurité et la confidentialité en ligne. De la loi sur la protection des données personnelles à la législation sur la cybercriminalité, nous plongerons dans les fondements essentiels de ce cadre juridique, examinant son importance pour assurer la confiance des individus, des entreprises et des institutions dans le monde numérique d'aujourd'hui.

1.1 L'arsenal juridique du cyberespace au Maroc

La cybersécurité est devenue un enjeu majeur dans notre société numérique en constante évolution. Afin de faire face aux menaces croissantes qui pèsent sur la sécurité des données et des systèmes informatiques, le Maroc a adopté la loi 05-20 relative à la cybersécurité. Cette loi joue un rôle essentiel dans la protection du paysage numérique marocain en établissant des mesures, des normes et des sanctions pour prévenir et contrer les attaques informatiques.

❖ La loi 05-20 relative à la cybersécurité

La loi 05-20 met l'accent sur la prévention et la réaction face aux cybermenaces. Elle définit les responsabilités des acteurs concernés, y compris les organismes gouvernementaux, les fournisseurs de services et les utilisateurs finaux. Cette législation met également en place des mécanismes de coordination et de coopération entre les différentes entités impliquées dans la sécurité des systèmes d'information, favorisant ainsi une approche holistique de la cybersécurité.

L'une des pierres angulaires de la loi 05-20 est la protection des données personnelles. Elle exige des entités publiques et privées de mettre en place des mesures de sécurité appropriées pour garantir la confidentialité, l'intégrité et la disponibilité des informations sensibles. De plus, la loi établit un cadre pour la notification des incidents de sécurité, obligeant les entités à signaler tout incident pouvant compromettre la sécurité des données personnelles.

La loi 05-20 accorde également une attention particulière à la prévention et à la répression des activités criminelles en ligne. Elle criminalise les actes tels que le piratage informatique, la fraude électronique, l'usurpation d'identité en ligne et d'autres formes de cybercriminalité. Des sanctions sévères sont prévues pour dissuader les individus ou les groupes de se livrer à de telles activités illégales.

Outre les mesures de prévention et de répression, la loi 05-20 met l'accent sur la sensibilisation et la formation en matière de cybersécurité. Elle encourage la mise en place de programmes de sensibilisation pour informer les utilisateurs finaux des risques liés à la sécurité en ligne et promeut la formation des professionnels de la cybersécurité pour renforcer les compétences

nécessaires dans ce domaine en constante évolution. Cette loi prévoit également des mécanismes de coopération internationale en matière de cybersécurité. Elle encourage la collaboration avec d'autres pays, les organisations internationales et les acteurs du secteur privé pour échanger des bonnes pratiques, partager des informations sur les menaces émergentes et coordonner les efforts dans la lutte contre la cybercriminalité à l'échelle mondiale.

En conclusion, la loi 05-20 relative à la cybersécurité constitue un pas important dans la protection du paysage numérique au Maroc. En établissant un cadre juridique solide, elle vise à renforcer la confiance des utilisateurs, à protéger les données personnelles et à prévenir les attaques informatiques. Cependant, il est important de souligner que la cybersécurité est un défi constant, car les attaques et les menaces évoluent rapidement. Par conséquent, la loi prévoit également des mécanismes d'évaluation et de mise à jour réguliers afin de s'adapter aux évolutions technologiques et aux nouvelles formes de cybermenaces.

Cette législation renforce également la coopération entre les secteurs public et privé dans le domaine de la cybersécurité. Elle encourage les partenariats entre les entités gouvernementales et les entreprises pour favoriser l'échange d'informations et la collaboration dans la détection et la réponse aux incidents de sécurité. Cette approche collaborative est cruciale pour renforcer la résilience du paysage numérique dans son ensemble. La loi 05-20 met également l'accent sur la protection des infrastructures critiques, telles que les systèmes d'énergie, de transport et de santé. Elle impose des normes de sécurité spécifiques et des mesures de protection renforcées pour garantir la continuité des services essentiels et la résistance face aux attaques potentielles.

Il convient de noter que la loi 05-20 ne se limite pas à la cybersécurité nationale, mais intègre également des dispositions relatives à la coopération internationale. Elle favorise la participation active du Maroc aux initiatives internationales visant à renforcer la cybersécurité à l'échelle mondiale, notamment en participant à des forums, des conférences et des programmes de partage d'informations.

En résumé, la loi 05-20 relative à la cybersécurité est une avancée majeure pour le Maroc dans la protection du paysage numérique contre les menaces en ligne. En établissant un cadre juridique solide, en promouvant la sensibilisation et la formation, et en encourageant la coopération nationale et internationale, cette législation vise à renforcer la confiance dans l'utilisation des technologies numériques et à assurer la protection des données, des infrastructures et des services essentiels.

1.1.1 L'arsenal juridique relative à l'échange électronique de données juridiques et aux services de confiance pour les transactions électroniques.

Le Maroc dispose d'un arsenal juridique relatif à l'échange électronique de données juridiques et d'une loi relative aux services de confiance pour les transactions électroniques.

La loi n° 53-05 réglemente la communication et la conservation des données électroniques dans les procédures judiciaires et administratives. Parallèlement, la loi n° 43-20 encadre la signature électronique et les services de confiance pour les transactions électronique. Ces textes visent à faciliter les échanges électroniques tout en assurant la sécurité et l'authenticité. Ils favorisent la confiance dans les transactions électroniques et encouragent la dématérialisation des procédures au Maroc. Dans cette partie, nous explorerons le cadre juridique relative à l'échange électronique de données juridiques, notamment la loi 53-05 et la loi 43-20 relative aux services de confiance pour les transactions électroniques.

❖ La loi 53-05 relative à l'échange électronique de données juridiques :

D'autre part on trouve que le législateur Marocain à renforcer son arsenal juridique par la loi 53-05, Cette loi fixe le régime applicable aux données juridiques échangées par voie électronique (cryptographie)[1] et à la signature électronique. Elle détermine également le cadre juridique applicable aux opérations effectuées par les prestataires de service de certification électronique, ainsi que les règles à respecter par ces derniers et les titulaires des certificats électroniques délivrés. La numérisation croissante de notre société a entraîné une transformation significative du domaine juridique. Afin de répondre aux besoins de ce nouveau paysage numérique, le Maroc a adopté la loi 53-05 relative à l'échange électronique de données juridiques. Cette loi vise à faciliter la transition vers le numérique dans le domaine juridique en établissant un cadre juridique pour la communication électronique, la conservation électronique des documents et les échanges électroniques de données juridiques.

La loi 53-05 reconnaît la validité juridique des documents électroniques, y compris les contrats, les notifications, les actes et les décisions judiciaires. Elle établit les conditions de leur échange électronique, en accordant une importance particulière à l'authenticité, l'intégrité et la confidentialité des données juridiques échangées. Cette législation définit également les modalités de conservation électronique des documents, garantissant leur valeur probante et leur

[1]La cryptographie est l'étude de la sécurité des communications grâce à l'utilisation de codes et de algorithmes pour protéger l'information de la divulgation non autorisée ou de la modification. La cryptographie joue un rôle crucial dans la protection de l'information confidentielle, telle que les données bancaires et les informations militaires, en les rendant illisibles pour les personnes malveillantes.

accessibilité à long terme. En mettant en place ce cadre juridique, la loi 53-05 encourage l'utilisation des technologies de l'information et de la communication dans le domaine juridique, ce qui permet d'améliorer l'efficacité, la rapidité et la sécurité des échanges de données. Elle favorise également la dématérialisation des procédures administratives et judiciaires, réduisant ainsi les coûts et les délais associés aux processus traditionnels.

La loi 53-05 impose également des exigences en matière de sécurité des données juridiques échangées électroniquement. Elle prévoit des mesures de protection appropriées pour prévenir les atteintes à la confidentialité et à l'intégrité des données, ainsi que des sanctions en cas de violation de ces obligations de sécurité. Cela contribue à renforcer la confiance dans l'échange électronique de données juridiques et à garantir la protection des droits des parties impliquées.

En outre, la loi 53-05 encourage la création de plateformes électroniques sécurisées pour faciliter les échanges de données juridiques entre les différentes parties. Ces plateformes permettent un accès centralisé aux documents, simplifient les procédures et favorisent la collaboration entre les acteurs du domaine juridique.

En conclusion, la loi 53-05 relative à l'échange électronique de données juridiques représente une étape importante dans la modernisation du domaine juridique au Maroc. En établissant un cadre juridique clair et sécurisé pour l'échange électronique de données, cette législation favorise l'efficacité, la rapidité et la sécurité des transactions juridiques. Elle ouvre également la voie à une transition vers le numérique, offrant de nouvelles opportunités pour les professionnels du droit et les citoyens. La loi 53-05 contribue à la simplification des procédures administratives et judiciaires, en réduisant les formalités et les contraintes liées aux documents papier. Grâce à l'échange électronique de données juridiques, les délais de traitement des dossiers peuvent être considérablement réduits, ce qui permet une justice plus rapide et plus accessible. De plus, la dématérialisation des documents juridiques facilite la gestion des archives et favorise une meilleure conservation des données dans le temps.

❖ La loi n° 43-20 relative aux services de confiance pour les transactions électroniques

La loi n° 43-20 relative aux services de confiance pour les transactions électroniques vise à établir le cadre réglementaire applicable aux différents aspects liés aux services de confiance pour les transactions électroniques. Cette loi aborde spécifiquement les services de confiance, les moyens et prestations de cryptologie, ainsi que les opérations réalisées par les prestataires de services de confiance et les règles qu'ils doivent respecter, tout comme les titulaires de certificats électroniques.

En détaillant les dispositions de cette loi, on trouve des mesures précises concernant la mise en place et la réglementation des services de confiance électronique. Cela englobe des services tels que l'horodatage, la signature électronique, l'authentification, la conservation électronique et la délivrance de certificats électroniques. De plus, la loi définit les règles et les exigences relatives aux moyens et prestations de cryptologie utilisés dans le cadre des transactions électroniques sécurisées. Elle établit les normes techniques, les procédures d'évaluation et de certification, ainsi que les obligations spécifiques pour les prestataires de services de confiance.

L'autorité nationale des services de confiance pour les transactions électroniques, telle que définie par la loi, se voit conférer des prérogatives importantes. Elle est chargée de superviser et de réguler les activités des prestataires de services de confiance, de délivrer des autorisations et de surveiller leur conformité aux règles établies. L'autorité joue également un rôle clé dans la certification des prestataires de services de confiance et la supervision de la sécurité des transactions électroniques.

En résumé, la loi n° 43-20 relative aux services de confiance pour les transactions électroniques a pour objectif de définir le cadre juridique et réglementaire visant à assurer la fiabilité, la sécurité et la validité des transactions électroniques à travers l'établissement de services de confiance et de normes de cryptologie. Elle confère également à l'autorité nationale des services de confiance un rôle central dans la supervision et la régulation de ces activités, garantissant ainsi la confiance des utilisateurs dans le domaine des transactions électroniques.

1.1.2 La protection des systèmes de traitement automatisé des données

Le Maroc à renforcer son arsenal juridique au niveau des systèmes de traitement automatisé des données par la loi n° 07-03, cette dernière constitue une étape décisive pour le Royaume. Il ne s'agit pas d'un texte s'appliquant uniquement à des cas bien définis mais d'une loi complétant le code pénale, elle couvre de nombreux agissements frauduleux imputables à l'informatique.

Les plus importantes incriminations contenues dans cette loi concernent les intrusions, ainsi que les atteintes aux systèmes de traitement automatisé des données.

- La loi 07-03 relative aux STAD[2]

Le législateur marocain a entrepris une démarche proactive par le biais de la loi 07-03 relative aux atteintes liées aux systèmes de traitement automatisé des données. Cette loi a été intégrée dans le code pénal marocain, aux articles 607-3 à 607-11.

[2] Système de Traitement Automatisé de Données.

En vertu de cette loi, des sanctions substantielles sont prévues pour toutes les infractions constituant des crimes contre les systèmes de traitement automatisé des données, proportionnellement à la gravité de l'infraction. Face à la problématique de la cybercriminalité, les approches légales diffèrent d'un pays à l'autre. Cela s'explique, en partie, par l'émergence de deux courants distincts, chacun adoptant une perspective différente de ce phénomène.

Le premier courant est d'avis qu'il n'est pas nécessaire d'établir une distinction entre les informations stockées sur des supports traditionnels et celles stockées de manière automatisée. Ainsi, la cybercriminalité ne justifie pas la mise en place de nouvelles mesures législatives.

Le deuxième courant considère la cybercriminalité comme un phénomène spécifique qui nécessite l'adoption de nouvelles mesures législatives. Les réponses juridiques marocaines s'inscrivent dans cette perspective, en reconnaissant la nécessité d'adopter des mesures spécifiques pour lutter contre ce phénomène en évolution constante.

1.2. L'arsenal juridique de la protection des données à caractère personnel

Au Maroc, la protection des données personnelles est réglementée par la loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, adoptée en 2009. Cette loi définit les principes fondamentaux pour le traitement des données personnelles, tels que le respect de la vie privée, la transparence, la responsabilité et la sécurité des données. Dans cette partie nous analysons l'efficacité et l'efficience de la loi 09-08 relative à la protection des données à caractère personnel.

❖ La loi 09-08 relative à la protection des données à caractère personnel

L'article 24 de la Constitution de 2011 sacralise le droit à la protection de la vie privée. En effet, la réforme constitutionnelle de juillet 2011 a réitéré la ferme volonté du Royaume du Maroc de bâtir un État de droit, démocratique et moderne, consacrant les droits de l'Homme ainsi que les libertés individuelles et collectives. Parmi ces derniers, le droit à la protection de la vie privée s'érige en un pilier fondamental.

La Constitution souligne ce droit fondamental en ces termes : « Toute personne a droit à la protection de sa vie privée…les communications privées, sous quelque forme que ce soit, sont secrètes. Seule la justice peut autoriser, dans les conditions et selon les formes prévues par la loi, l'accès à leur contenu, leur divulgation totale ou partielle ou leur invocation à la charge de quiconque…». (L'article 24 de la constitution Marocaine de 2011).

La Constitution vise à garantir les droits des individus sur les informations personnelles en affirmant le principe de protection de la vie privée.

Dans ce cadre le législateur Marocain a instauré la loi marocaine 09-08 relative à la protection des données à caractère personnel pour but de protéger les droits fondamentaux des individus en ce qui concerne le traitement de leurs informations personnelles. Cette législation établit les responsabilités des responsables du traitement des données, les droits des personnes concernées, ainsi que les sanctions en cas de non-respect. Selon cette loi, les données doivent être collectées de manière légale, transparente et proportionnée, et les individus doivent être informés de la finalité du traitement de leurs données. La loi exige également que les données soient sécurisées et protégées contre tout accès non autorisé. Les personnes concernées ont le droit d'accéder à leurs données, de les rectifier ou de les supprimer. Des sanctions sont prévues pour les infractions telles que la collecte illégale de données, la violation de la vie privée ou le non-respect des normes de protection des données. En résumé, la loi 09-08 vise à assurer la protection de la vie privée et des données personnelles dans un environnement numérique en constante évolution.

L'utilisation des données personnelles nécessite une base juridique solide et des dispositions visant à protéger les utilisateurs contre toute violation de leurs données et de leur vie privée, afin de leur inspirer confiance dans les technologies de l'information et de la communication.

Une donnée à caractère personnel est toute information permettant d'identifier directement ou indirectement une personne physique. Selon la définition juridique, il s'agit de toute information liée à une personne physique identifiée ou identifiable, pouvant être directement ou indirectement identifiée grâce à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou d'autres éléments spécifiques d'ordre économique, culturel ou social. Le législateur marocain a également défini la donnée à caractère personnel dans l'article 1 de la loi 09-08. Selon cette définition, il s'agit de toute information, quelle que soit sa nature et son support, y compris le son et l'image, concernant une personne physique identifiée ou identifiable, désignée comme la "personne concernée". Une personne est considérée comme identifiable si elle peut être directement ou indirectement identifiée, notamment par le biais d'un numéro d'identification ou d'éléments spécifiques liés à son identité physique, psychologique, génétique, économique, culturelle ou sociale.

Les données à caractère personnel regroupent des informations numériques liées à une personne, telles que son nom, son prénom, sa photographie, sa date de naissance, son numéro de carte bancaire, son numéro de sécurité sociale, ses empreintes digitales, sa voix, etc. Parfois, ces données sont qualifiées de "données sensibles", désignant des informations à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions

religieuses ou philosophiques, ou l'appartenance syndicale de la personne concernée, ainsi que les données relatives à sa santé, y compris les données génétiques. La collecte, l'enregistrement, la conservation, l'extraction, la communication, la transmission, la diffusion, le rapprochement, l'interconnexion, l'effacement ou la destruction de ces informations personnelles constituent des actions relatives à ces données.

2. Le cadre institutionnel de la protection des données personnelles au Maroc :

le Maroc dispose d'un cadre institutionnel robuste pour la protection des données personnelles. Grâce à des organismes tels que la Direction Générale de la Sureté Nationale, la Commission Nationale de contrôle de la protection des Données à caractère Personnel et la Direction Générale de la Sécurité des Systèmes d'Information. Le pays s'engage à préserver la confidentialité, la sécurité et les droits fondamentaux des individus dans le monde numérique. Ce cadre institutionnel renforce la confiance des individus dans l'utilisation des services numériques et contribue à la promotion d'un environnement numérique sûr et responsable au Maroc.

❖ La direction générale de la sureté nationale.

Sur le plan organisationnel, deux services distincts ont été établis afin de lutter contre la criminalité associée aux nouvelles technologies de l'information ainsi que la cybercriminalité. Le premier service est pourvu d'un laboratoire central des traces numériques, dédié à l'expertise des supports numériques saisis par les services de police à l'échelle nationale.

Quant au deuxième service, il relève de la brigade nationale de la police judiciaire et dispose également de son propre laboratoire d'exploitation des traces numériques. En outre, la Direction Générale de la Sûreté Nationale compte 29 brigades spécialisées dans la lutte contre la cybercriminalité, dont quatre possèdent leurs propres laboratoires à Casablanca, Fès, Marrakech et Laâyoune.

Dans la lutte contre la cybercriminalité, l'élément humain formé et bien encadré demeure d'une importance capitale. Afin de s'adapter en permanence à l'évolution de ce phénomène, la Police nationale marocaine a procédé au recrutement de profils de qualité.

Les équipes composant les différentes brigades sont constituées d'ingénieurs, de techniciens spécialisés, d'analystes, de juristes, ainsi que d'autres professionnels dont l'expertise renforce les actions menées dans ce domaine. Le gouvernement s'engage à renforcer la formation afin d'accroître la vigilance nécessaire face aux dangers de la cybercriminalité

❖ **La DGSSI [3]**

Au Royaume du Maroc, à l'image de la France, la Direction Générale de la Sécurité des Systèmes d'Information a été établie au sein de l'Administration de la Défense Nationale. Elle est placée sous l'autorité de l'Administration de la Défense Nationale du Royaume du Maroc. Les attributions de cette direction portent sur la prévention et la détection des attaques informatiques.

La DGSSI est chargée de coordonner les travaux interministériels relatifs à l'élaboration et à la mise en œuvre de la stratégie de l'État en matière de sécurité des systèmes d'information. Elle veille à l'application des directives et orientations du comité stratégique de la sécurité des systèmes d'information, propose des normes et des règles spécifiques à la sécurité des systèmes d'information de l'État, délivre des autorisations et gère les déclarations liées aux moyens et aux prestations de cryptographie. La DGSSI est également responsable de la certification des dispositifs de création et de vérification de signature électronique. Elle agrée les prestataires de services pour la certification électronique conformément aux dispositions légales. Elle assiste et conseille les administrations, les organismes publics et le secteur privé dans la mise en place de la sécurité de leurs systèmes d'information.

En outre, la DGSSI développe l'expertise scientifique et technique dans le domaine de la sécurité des systèmes d'information. Elle réalise des audits de sécurité des systèmes d'information des administrations et des organismes publics. Elle met en place un système de veille, de détection et d'alerte des événements impactant la sécurité des systèmes d'information de l'État et coordonne les mesures à prendre en conséquence.

En situation d'urgence ou de menace, la DGSSI saisit le comité stratégique de la sécurité des systèmes d'information et assure une veille technologique afin d'anticiper les évolutions et de proposer les innovations nécessaires en matière de sécurité des systèmes d'information.

❖ **La Commission Nationale de contrôle de la protection des Données à caractère Personnel.**

La Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel a été établie en vertu de la loi 09-08 du 18 février 2009. Sa mission principale consiste à mettre en œuvre et à garantir le respect des dispositions de ladite loi ainsi que des autres textes de référence régissant la protection des données personnelles.

[3] La Direction générale de la sécurité des systèmes d'informations.

La CNDP mène des actions de sensibilisation auprès des individus, des organismes, et des institutions publiques et privées, dans le but de renforcer leur connaissance des droits et obligations en matière de protection des données personnelles. Dans ce cadre, la CNDP met à disposition un portail électronique régulièrement mis à jour, élabore des brochures d'information, produit des spots pour la radio et la télévision, ainsi qu'une émission radio hebdomadaire. De plus, la CNDP accompagne les acteurs concernés dans l'alignement de leurs procédures de traitement des données personnelles. Une attention particulière est accordée aux secteurs traitant une quantité significative de données personnelles.

La CNDP a pour rôle de conseiller les acteurs publics impliqués dans le domaine de la protection des données personnelles tels que le gouvernement, le parlement et l'administration. Elle peut émettre des avis sur les projets de lois et de règlements, proposer des législations au gouvernement et contribuer à la préparation de la position du Maroc lors des négociations internationales sur ce sujet. La CNDP est également chargée de traiter les plaintes des citoyens relatives aux violations de leurs droits à la protection des données personnelles. La majorité des plaintes concerne des problématiques telles que la publicité abusive, les spams, la vidéosurveillance. Par ailleurs, la CNDP traite les déclarations et les demandes d'autorisation émanant des responsables de traitement des données personnelles. Elle peut accorder des autorisations pour la conservation des données au-delà de la durée prévue et délivrer des autorisations de traitement pour des catégories spécifiques de données considérées comme sensibles.

Enfin, la CNDP est responsable du registre national de la protection des données personnelles qui recense, entre autres, la liste des fichiers traités par les autorités publiques ainsi que les autorisations de traitement accordées. La CNDP dispose de pouvoirs d'investigation et d'enquête lui permettant de contrôler et de vérifier la conformité des traitements des données personnelles avec la loi.

2.1. Les mesures prises par les sociétés de traitement et leurs obligations en matière de protection des données personnelles

Les entreprises chargées du traitement des données mettent en œuvre des mesures essentielles pour assurer la protection des informations sensibles. Face aux menaces croissantes en matière de cybersécurité, ces entreprises appliquent des protocoles de sécurité stricts afin de garantir la confidentialité, l'intégrité et la disponibilité des données. En adoptant des politiques de confidentialité solides, des méthodes de cryptage avancées, des systèmes d'authentification

renforcés et des procédures régulières de sauvegarde, elles visent à prévenir les violations de données et à protéger leurs clients contre les risques potentiels. Cette partie explorera les différentes mesures prises par les responsables de traitement des données pour assurer la sécurité des informations confidentielles dont elles ont la charge.

❖ Les obligations des responsables de traitement en matière de protection des données personnelles :

La loi marocaine 09-08 relative à la protection des données personnelles réglemente le traitement des données personnelles. Elle établit les obligations des responsables de traitement et des sous-traitants en matière de protection des données personnelles. Voici les principales obligations décrites par cette loi :

- Respect de la légalité : Les responsables de traitement doivent se conformer aux lois et réglementations en vigueur, y compris le RGPD[4] en Europe et la loi marocaine 09-08.
- Finalité limitée : Les données personnelles ne doivent être traitées que dans un but spécifique, explicite et légitime, et ne doivent pas être utilisées à d'autres fins que celles pour lesquelles elles ont été collectées.
- Minimisation des données : Les responsables de traitement doivent collecter uniquement les données nécessaires à la réalisation des fins pour lesquelles elles ont été collectées.
- Exactitude des données : Les responsables de traitement doivent s'assurer que les données qu'ils traitent sont exactes et à jour, et prendre les mesures nécessaires pour corriger ou supprimer les données inexactes.
- Stockage sécurisé : Les responsables de traitement doivent mettre en place des mesures de sécurité appropriées pour protéger les données personnelles qu'ils traitent, en veillant à les stocker de manière sécurisée.
- Transparence : Les responsables de traitement doivent informer les personnes concernées des modalités de traitement de leurs données personnelles et de leurs droits en matière de protection des données.
- Respect des droits des personnes concernées : Les responsables de traitement doivent respecter les droits des personnes concernées, tels que le droit d'accès, de rectification, d'effacement et de portabilité de leurs données personnelles.

Il est essentiel que les responsables de traitement et les sous-traitants respectent ces obligations afin de garantir la protection des données et le respect des droits des personnes concernées. Les

[4] Le Règlement Général sur la Protection des Données est un texte réglementaire européen qui encadre le traitement des données de manière égalitaire sur tout le territoire de l'Union européenne (UE).

sociétés de traitement des données jouent un rôle crucial dans cette protection en mettant en place différentes mesures, notamment :

- Établissement de politiques de confidentialité claires et transparentes pour informer les utilisateurs sur la collecte, l'utilisation, le stockage et la protection de leurs données personnelles, ainsi que sur leurs droits de contrôle des données.
- Mise en place de mesures de sécurité techniques et organisationnelles pour protéger les données personnelles contre tout accès, utilisation, divulgation ou altération non autorisés.
- Contrôle strict de l'accès aux données personnelles en limitant l'accès aux employés autorisés et en utilisant des protocoles d'authentification robustes.
- Formation du personnel sur les meilleures pratiques de protection des données et de cybersécurité.
- Réalisation d'audits internes pour évaluer l'efficacité des mesures de protection des données.
- Gestion stricte des fournisseurs et des sous-traitants pour s'assurer de leur conformité aux normes de sécurité.
- Mise en place de procédures de réponse aux incidents de sécurité, y compris la notification des violations de données aux autorités compétentes et aux personnes concernées.

Les sociétés de traitement des données doivent également effectuer des évaluations régulières des risques, protéger les données sensibles, gérer le cycle de vie des données, collaborer avec les autorités compétentes, sensibiliser les utilisateurs et prendre d'autres mesures pour renforcer la protection des données personnelles dans le cyberespace. Cependant, la protection des données personnelles ne relève pas seulement de la responsabilité des entreprises, mais aussi des individus, des gouvernements et des autres acteurs impliqués. Une approche collective et une collaboration étroite sont nécessaires pour relever les défis complexes de la protection des données personnelles et de la cybersécurité.

2.2. Les obligations des gouvernements

Le gouvernement marocain doit s'assurer d'adopter des pratiques transparentes et responsables dans l'utilisation des données personnelles en vue de la protection de la nation. A cet égard, il est nécessaire de :

- ✓ Limiter la collecte de données : Le gouvernement doit veiller à ne collecter que les données strictement nécessaires à la protection de la nation, en s'assurant que les données collectées soient pertinentes, fiables et à jour.

- ✓ Assurer la protection des données : Le gouvernement doit mettre en place des mesures de sécurité afin de protéger les données personnelles contre les fuites, les pertes ou les abus. Ces mesures peuvent comprendre le chiffrement des données, la formation du personnel sur les bonnes pratiques de sécurité et l'établissement de politiques de sécurité rigoureuses.
- ✓ Respecter la vie privée : Le gouvernement doit respecter les droits des citoyens à la vie privée et à la protection de leurs données personnelles. Cela peut impliquer la mise en place de procédures visant à obtenir le consentement éclairé des citoyens avant la collecte de données, ainsi que la mise en place de mécanismes de contrôle permettant aux citoyens de surveiller l'utilisation de leurs données.
- ✓ Transparence : Le gouvernement doit faire preuve de transparence concernant les activités de collecte, de stockage et d'analyse des données personnelles. Cela peut inclure la publication régulière de rapports sur les activités de collecte de données, la fourniture d'informations sur les politiques de collecte de données aux citoyens et la mise en place de mécanismes permettant aux citoyens de faire des enquêtes sur l'utilisation de leurs données.

En adoptant ces pratiques responsables et transparentes, le gouvernement peut renforcer la confiance des citoyens dans l'utilisation des données personnelles pour la protection de la nation, tout en veillant à ce que cette utilisation soit conforme aux dispositions de la loi 09-08 sur la protection des données personnelles. Ceci contribue à garantir que le gouvernement utilise les données de manière légitime et responsable pour la protection de la nation, tout en préservant les droits fondamentaux des citoyens à la vie privée et à la protection de leurs données personnelles. En conclusion, l'utilisation des données personnelles par les gouvernements pour la protection de leur pays est une question complexe qui nécessite un équilibre entre la protection de la sécurité nationale et la préservation des droits fondamentaux des citoyens.

2.3. L’utilisateur au centre de la cyber sécurité

Dans l’optique de préserver et protéger les droits et les libertés fondamentaux des utilisateurs du cyberespace, la loi 09-08 relative à la protection des données à caractère personnel garantit certains droits de la personne concernée.

❖ Les droits de la personne concernée :

- Droit de l’information lors de la collecte des données à caractère personnel : Selon l’article 6 de la loi 09-08 une information expresse et non équivoque sauf s’il y des limites c’est-à-

dire lors de la collecte des données la personne concernée a le droit de savoir si une telle question est obligatoire ou facultative.

- L'obligation de consentement : Un traitement de données à caractère personnel doit avoir le consentement de la personne concernée. L'article 4 de la loi 09-08 dispose que la communication des données à caractère personnel à un tiers nécessite indubitablement le consentement préalable de la personne concernée. Le premier article de la loi précitée 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. Il y a des exceptions à cette obligation lorsqu'il s'agit d'une exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique.
- Droit d'accès : Le droit d'accès tel que reconnu à l'article 7 de la loi 09-08 est le droit que permet à toute personne d'accéder aux information la concernant pour s'assurer de l'exactitude. La personne concernée a le droit d'obtenir du responsable du traitement les informations concernant les finalités du traitement. Ce droit n'est pas absolu : le responsable du traitement n'est pas tenu de répondre à des demandes manifestement abusives, dans ce cas, il doit informer la Commission Nationale en apportant la preuve du caractère abusif de ces demandes.
- Droit de rectification :Droit pour tout individu de faire rectifier, compléter, actualiser, verrouiller, effacer des informations les concernant. Ce droit complète le droit d'accès et il permet aux personne concernées d'exercer la rectification des informations, notamment lorsqu'ils sont inexacts ou incomplets. Ce droit s'exerce par le biais d'une requête adressée au responsable du traitement qui tenu du répondre dans un délai de 10 jours sans imposer de frais.
- Droit d'opposition : Droit pour tout individu de s'opposer à ce que des données personnelles à caractère personnel qui la concernant fassent l'objet d'un traitement. Le droit d'opposition d'une personne au traitement de ses données fait partie des principes fondamentaux de protection de la vie privée et des liberté publiques. Ce droit n'est pas absolu, son exercice n'est possible, de manière générale, que pour « motif légitime ». Selon la loi 09-08 et selon son article 9 qui permet à toute personne dont les données à caractère personnel font l'objet d'un traitement de s'opposer à ce que ces données soient utilisées à des fins de protection surtout commerciale.

- Le droit à l'oubli : Le droit à l'oubli est un droit spécifique qui concerne uniquement les moteurs de recherche. Il consiste à supprimer ou à éliminer les résultats de moteurs de recherche, en cas de refus, il doit y avoir une plainte auprès de la CNDP. En tout cas il est difficile d'être sûr qu'une donnée peut être effacée sur internet, parce qu'elle peut être sauvegardée par d'autre utilisateurs ou autres moteurs de recherche. Avec toutes les efforts du monde entiers de l'exigence et l'obligation de la protection des données à caractère personnel il y a toujours des violations à ces données par le biais de la technologie avancé et les criminels qui utilisent de plus en plus des outils de communications électroniques pour préparer, organiser et mettre en œuvre leurs actions. Il y a aussi, droit à la portabilité des données, droit à obtenir réparation etc…

D'importantes tentatives ont été faites pour contrôler la croissance naissante des nouvelles technologies afin de sauvegarder et d'améliorer continuellement la vie sacrée de l'individu. Comme nous venons de le voir, il existe une base pour la protection des données personnelles, permettant aux utilisateurs des nouvelles technologies de protéger leurs droits, leurs droits et leur vie privée, qui sont considérés comme des droits légaux de toute personne, indépendamment de sa race ou de son pays. Cependant, la question va au-delà de l'échange pour des raisons économiques, car le gouvernement affirme que la sécurité de son pays prime sur la protection de la vie privée. Même si les nouvelles technologies se développent rapidement, d'importants efforts juridiques et sociétaux sont déployés pour suivre et intégrer cette évolution dans le domaine de la protection des données personnelles.

❖ **Des mesures préventives pour sécuriser les données personnelles dans le cyber espace.**

Utiliser internet c'est donner aux cybercriminels la main sur nos données personnelles qui sont de réelles mines d'or, en tente d'ailleurs ne jamais utiliser cet outil qu'est devenu indispensable dans notre vie, utiliser internet pour faire des courses, des achats, des cours à distance, des recherches scientifiques, des conseils, c'est l'omniprésence du système d'information.

Il faut donc s'avoir se protéger et pas s'enfuir, à côté des instances de protection comme la Commission National de l'Informatique et des libertés en France, la CNDP, la DGSN et la DGSSI au Maroc qui pour but d'encadrer tout organisme traitant des données personnelles et s'assurer à ce que le règlement soit respecté.

L'utilisateur est tenu à respecter et d'appliquer quelques normes pour éviter l'exploitation de ses données personnelles et pour éviter les attaques dans le cyberespace, notamment le chiffrement des données, l'utilisation des mots de passes forts, tenue à jour des logiciels, éviter

les réseaux Wi-Fi publics non sécurisés, attention aux e-mails de phishing, l'utilisation de logiciels de sécurité et la sauvegarde régulière des données. [IFRAH L., (2010). L'Information et le renseignement par Internet. Comment gérer l'information à l'heure du Web 2.0 ?].

Conclusion :

La protection des données personnelles et la cybersécurité revêtent une importance primordiale dans l'évolution constante du paysage numérique au Maroc. Le pays a entrepris des mesures significatives pour établir un cadre juridique solide ainsi qu'un dispositif institutionnel efficace en vue de garantir la confidentialité, l'intégrité et la sécurité des données personnelles dans le contexte d'une expansion numérique en plein essor.

La loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel constitue l'un des piliers fondamentaux du cadre juridique marocain en matière de protection des données. Cette législation a été conçue pour établir les principes fondamentaux régissant la protection des données personnelles et encadrer leur collecte, leur traitement, leur stockage et leur transfert. Son objectif est de garantir le respect des droits individuels en matière de protection des données, tout en exigeant des responsables du traitement des données qu'ils adhèrent à des normes rigoureuses de sécurité et de confidentialité. Parallèlement, la loi 53-05 relative à l'échange électronique de données juridiques vise à sécuriser les échanges électroniques et à promouvoir l'utilisation des technologies de l'information et de la communication. Cette législation revêt une importance cruciale pour faciliter les transactions électroniques et renforcer la confiance dans l'économie numérique en garantissant la sécurité des échanges de données juridiques.

En vue de superviser et de contrôler la mise en œuvre des mesures de protection des données, le Maroc dispose d'institutions clés telles que la Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel. La CNDP joue un rôle essentiel dans la surveillance, la réglementation et la sensibilisation à la protection des données, veillant à ce que les entreprises et les organisations respectent les obligations légales en matière de protection des données et mettent en place des mesures de sécurité adéquates.

Malgré les progrès significatifs réalisés par le Maroc en matière de protection des données personnelles et de cybersécurité, des défis persistent. Une sensibilisation accrue aux enjeux de la protection des données est essentielle pour éduquer les individus sur leurs droits et les bonnes pratiques en matière de confidentialité et de sécurité. De plus, la mise en œuvre effective des

mesures de sécurité et la coordination entre les différentes parties prenantes restent des aspects critiques à améliorer.

Afin de renforcer davantage la protection des données personnelles et la cybersécurité, le Maroc doit poursuivre ses efforts en renforçant son cadre juridique et en améliorant les mécanismes de supervision et de contrôle. Il est également essentiel de promouvoir une culture de la cybersécurité à tous les niveaux de la société en encourageant la sensibilisation, la formation et la collaboration entre les institutions gouvernementales, le secteur privé et la société civile. La coopération et la coordination entre ces acteurs sont indispensables pour faire face aux défis complexes et en constante évolution liés à la protection des données personnelles et à la cybersécurité.

En renforçant son cadre juridique, le Maroc doit également s'adapter aux développements technologiques rapides ainsi qu'aux nouvelles menaces cybernétiques. Les lois et réglementations doivent être régulièrement révisées et mises à jour pour tenir compte des avancées technologiques et des défis émergents. Cela garantira une protection efficace des données personnelles et une cybersécurité robuste dans un environnement numérique en constante évolution. La confiance des individus dans l'utilisation des services numériques constitue un élément clé pour favoriser le développement de l'économie numérique au Maroc. Les citoyens doivent avoir l'assurance que leurs données personnelles sont traitées de manière sécurisée et confidentielle. Cela nécessite la mise en place de mesures de sécurité solides, d'une transparence accrue de la part des organisations traitant les données, ainsi que de mécanismes de contrôle et de recours en cas de violation de la vie privée. Parallèlement, la promotion d'une culture de la cybersécurité est essentielle pour sensibiliser les individus aux risques liés à la protection des données et aux meilleures pratiques de sécurité. La sensibilisation doit s'étendre à tous les niveaux, que ce soit au sein des organisations, dans les établissements d'enseignement, ou à travers des campagnes de sensibilisation publiques. Les citoyens doivent être informés des menaces potentielles, des mesures de prévention et des actions à prendre en cas d'incident de sécurité.

En conclusion, la protection des données personnelles et la cybersécurité représentent des enjeux majeurs au Maroc, nécessitant une attention continue et des efforts coordonnés. Le pays a mis en place un cadre juridique et institutionnel solide afin d'assurer la confidentialité, l'intégrité et la sécurité des données personnelles. Toutefois, des défis subsistent, notamment en termes de sensibilisation, de mise en œuvre des mesures de sécurité et de coordination entre les différentes parties prenantes. En renforçant son cadre juridique, en promouvant une culture

de la cybersécurité et en favorisant la collaboration entre les acteurs concernés, le Maroc peut consolider sa position en tant que pays numérique sûr et fiable. Cela favorisera le développement de l'économie numérique, renforcera la confiance des individus dans l'utilisation des services numériques et garantira la protection des données personnelles dans un monde numérique en constante évolution.

BIBLIOGRAPHIE

➢ ***Ouvrages généraux :***

- IFRAH L., (2010). L'Information et le renseignement par Internet. Comment gérer l'information à l'heure du Web 2.0 ?, Que sais-je ?, n° 3881, PUF.
- LEPAGE A., (2002). Libertés et droits fondamentaux à l'épreuve de l'Internet : droits de l'internaute, liberté d'expression sur l'Internet, responsabilité, Litec.

➢ **Ouvrages spéciaux :**

- Association des Utilisateurs des Systèmes d'Information au Maroc en collaboration avec la société SOLUCOM, Livre Blanc Données à caractère personnel : Quels enjeux et comment se préparer à la loi 09-08 ?
- BANCK AURELIE, (2019). RGPD : la protection des données à caractère personnel : Intègre l'ordonnance adaptant la loi Informatique et Libertés Ed.2, Editeur Gualino.
- FABRICE MATTATIA, RGPD ET DROIT DES DONNÉES PERSONNELLES, (2018). Enfin un manuel complet sur le nouveau cadre juridique issu du RGPD et de la loi Informatique et libertés, 3éme édition.

➢ **Thèses et mémoires :**

- HAOUNANI, A. (2019). L'UTILISATION DES DONNEES PERSONNELLES DANS LE DROIT COMPARE, Mémoire pour l'obtention du Master Droit Du Numérique, soutenue en 2019. Faculté des sciences juridiques et politiques- université Hassan premier Settat/ Maroc.
- NATHALIE WALCZAK, (2014). La protection des données personnelles sur l'internet : Analyse des discours et des enjeux sociopolitiques. Thèse de doctorat en Sciences de l'information et de la communication Sous la direction d'Isabelle GARCIN-MARROU et de Franck REBILLARD.

➢ **Articles :**

- HAOUNANI, .A. & AKKOUR, .S. (2023). LES DONNÉES PERSONNELLES À L'ÈRE DU BIG-DATA : QUEL CADRE JURIDIQUE AU MAROC ?. *Revue Internationale du chercheur*. 4, 1.

➢ **Rapports :**

- PROTECTION DES DONNEES PERSONNELLES - ANALYSE COMPAREE DES LEGISLATIONS ET DES PRATIQUES /DANS NEUF PAYS EUROPEENS - dans le contexte du cadre juridique européen.
- Rapport sur la protection des données personnelles dans le cadre du secteur de la sécurité au Maroc/ Séminaire. (2015). DCAF-CEDHD - Rabat, Maroc.

➢ **Webographie :**

- Site officiel de la CNDP, consultable sur https://www.cndp.ma/fr/cndp/qui-sommes-nous/commision.html
- Site officiel de la CNIL, consultable sur https://www.cnil.fr/fr/reglement-europeen-protection-donnees
- Le site officiel de la DGSSI, consultable sur le lien suivant : https://www.dgssi.gov.ma/fr/presentation/dgssi/presentation-missions.html