مركز دراسات حقوق الإنسان والديموقراطية

ⵓⵔⵔⴰⵡ ⵏⵜⵙⵔⴰⵔⵉⵏ ⵏ ⵜⵣⵔⴼⵜ ⴷ ⵜⵎⵓⴽⵔⴰⵟⵉⵜ

Centre d'Etudes en Droits Humains et Démocratie

DCAF

un centre pour la sécurité,
le développement et
l'état de droit

Rapport

La Protection Des Données Personnelles
Dans Le Cadre Du Secteur De La Sécurité Au Maroc

Séminaire DCAF - CEDHD

19 et 20 octobre 2015 – Rabat, Maroc

Avec le soutien financier
du Fonds d'affection du DCAF
pour l'Afrique du Nord

DCAF TRUST FUND FOR NORTH AFRICA

Rapport

LA PROTECTION DES DONNÉES PERSONNELLES DANS LE CADRE DU SECTEUR DE LA SÉCURITÉ AU MAROC

Séminaire DCAF - CEDHD
19 et 20 octobre 2015 – Rabat, Maroc

À propos du Centre pour le contrôle démocratique des forces armées – Genève (DCAF)

Le Centre pour le contrôle démocratique des forces armées – Genève (DCAF) est une organisation internationale basée en Suisse et comprenant actuellement 63 États-membres. Le DCAF assiste des États – qu'il s'agisse de démocraties établies ou émergentes – dans le développement de la bonne gouvernance du secteur de la sécurité au sein d'un cadre démocratique et dans le respect de l'état de droit. Le DCAF fournit également un appui consultatif et des programmes d'assistance pratique à des États visant à renforcer la gouvernance de leur secteur de la sécurité. Le DCAF travaille directement avec des gouvernements nationaux et locaux, des parlements, des organisations internationales, la société civile ainsi qu'avec les forces de sécurité et de défense.

Dans ses activités, le DCAF est guidé par les principes de neutralité, d'impartialité, de participation inclusive et d'appropriation locale.

De plus amples informations sur le DCAF et ses activités sont disponibles sur le site web du DCAF: **www.dcaf.ch** ou sur le site web du DCAF en Tunisie: **www.dcaf-tunisie.org**

À propos du Centre d'études en droits humains et en démocratie

Le Centre d'Études en Droits Humains et Démocratie (CEDHD) est une organisation non gouvernementale à but non lucratif, spécialisée et indépendante des pouvoirs publics et des courants politiques. Il a été créé en 2005, sur la base des expériences acquises par nombre de ses membres fondateurs au sein d'institutions gouvernementales et non gouvernementales et organismes universitaires œuvrant en matière des droits humains.

La création du CEDHD est une contribution au suivi de l'évolution de la situation des droits humains au Maroc et ailleurs dans sa relation avec le processus de construction démocratique, et l'analyse des modalités de la consécration de ce choix au niveau des politiques publiques.

De plus amples informations sur le CEDHD sont disponibles sur le site web du CEDHD: **www.cedhd.org**

À propos de ce rapport

Ce rapport présente un résumé des discussions menées lors du séminaire. Sa publication vise d'une part à faire le point sur la protection des données personnelles dans le cadre du secteur de la sécurité au Maroc. D'autre part, il a pour objectif de sensibiliser les acteurs concernés à l'importance de la protection de la vie privée des citoyens en tant qu'enjeu majeur de la gouvernance sécuritaire dans les sociétés connectées.

Remerciements

Ce projet a été réalisé avec le soutien financier des Etats membres du Fonds d'affectation du DCAF pour l'Afrique du Nord (TFNA). Pour plus d'informations au sujet du TFNA veuillez consulter le site web: **www.dcaf-tfna.org.**

Le DCAF et le CEDHD remercient également tous les participants au séminaire des 19 et 20 octobre 2015 pour leurs riches interventions.

Comité de rédaction

Cécile Guy, DCAF Genève
Alizée Henry, DCAF Genève
Habib Belkouch, CEDHD

ISBN: 978-92-9222-411-0

TABLE DES MATIÈRES

INTRODUCTION

La généralisation de l'informatique et de l'internet, ainsi que le développement rapide des réseaux sociaux et des objets interconnectés (tablettes, smartphones, GPS), ont accru l'échange et le partage de données à caractère personnel. Au Maroc, le taux de pénétration d'internet dépassait les 30% et celui de la téléphonie mobile culminait à plus de 130 % en 2014. D'un côté, cette évolution est synonyme de nouvelles opportunités et de services innovants. De l'autre, elle comporte des risques pour la vie privée, les libertés et droits fondamentaux de l'individu, ainsi que pour la sécurité de l'Etat et de la société.

En effet, la rapidité, la commodité et l'anonymat de la toile sont souvent exploités à des fins illégales, voire criminelles. Afin de prévenir et de lutter contre ces agissements, de nombreux Etats optent pour des politiques de surveillance électronique. Les services de sécurité sont donc de plus en plus amenés à collecter, stocker et le traiter certaines données à caractère personnel[1].

L'utilisation de ces méthodes par nature intrusives doit être soumise à un cadre légal clair et adéquat, afin d'en assurer une mise en œuvre transparente, non-abusive et non-arbitraire. Il s'agit de savoir comment bénéficier des biens et services innovants de l'ère numérique et de permettre aux services de sécurité de remplir leur mission, sans toutefois porter atteinte aux droits et libertés des individus. Or, comme l'ont révélé certains lanceurs d'alertes, ce cadre est encore imparfait dans de nombreux pays.

Au cours des dernières années, le Maroc s'est positionné en faveur d'une meilleure protection des citoyens contre l'usage abusif du traitement automatisé des données à caractère personnel.

Le Royaume a notamment :

- créé la Commission Nationale de contrôle de la protection des Données à caractère Personnel (CNDP),
- instauré la Direction générale de la sécurité des systèmes d'information (DGSSI) qui est l'autorité en charge de la sécurité cybernétique,
- ratifié la Convention 108 du Conseil de l'Europe et son protocole additionnel[2].

Afin que le pays respecte ses engagements internationaux, une mise à niveau juridique et institutionnelle semble indispensable.

Les 19 et 20 octobre 2015, le Centre pour le contrôle démocratique des forces armées - Genève (DCAF) et le Centre d'Etudes en Droits Humains et Démocratie (CEDHD) ont organisé à Rabat un séminaire sur le thème de «La bonne gouvernance du secteur de la sécurité à l'ère numérique: gestion et protection des données personnelles».

Cet événement visait à:

- échanger les expériences et offrir une expertise internationale en matière de gestion et protection des données personnelles,

1. L'article 2 de la Convention 108 du Conseil de l'Europe relative à la protection des personnes à l'égard du traitement automatisé des données à caractère personnel définit une donnée personnelle comme suit : « toute information concernant une personne physique identifiée ou identifiable («personne concernée») ».
2. Voir présentation de la Convention page 11.

- analyser le champ d'application de la loi 09-08 relative à la protection des personnes physiques à l'égard du traitement de leurs données personnelles par les services de sécurité,
- déterminer les interactions entre les acteurs du secteur de sécurité et la gestion et protection des données personnelles au Maroc
- identifier les implications de l'adhésion du Maroc à la Convention 108 du Conseil de l'Europe et à son Protocole additionnel et son protocole additionnel pour le secteur de la sécurité et pour le cadre juridique de la protection des données.

Une cinquantaine de participants marocains et internationaux ont pris part aux discussions, dont notamment des représentants des autorités exécutives, législatives et judiciaires, des services de sécurité, de la CNDP, des médias et de la société civile, ainsi que des experts internationaux.

Ce rapport présente un résumé des discussions menées lors du séminaire. Sa publication vise d'une part à faire le point sur la protection des données personnelles dans le cadre du secteur de la sécurité au Maroc. D'autre part, il a pour objectif de sensibiliser les acteurs concernés à l'importance de la protection de la vie privée des citoyens en tant qu'enjeu majeur de la gouvernance sécuritaire dans les sociétés connectées.

A. Bonne gouvernance du secteur de la sécurité et protection des données personnelles

1. Concilier impératifs sécuritaires et protection de la vie privée à l'ère numérique

La «mise en données» de la société

L'importance des nouvelles technologies de la communication et de l'information (NTIC) s'est amplifiée au cours des dernières décennies. Les NTIC et leurs opérateurs sont devenus indispensables aux individus, tout comme aux Etats et à leurs économies. L'informatisation des sociétés a notamment permis d'augmenter la rapidité des processus de production et d'administration, de faciliter les communications aux niveaux national et international ou encore de résoudre certains problèmes liés au stockage de l'information. Dans le cadre du secteur de la sécurité, les nouvelles technologies ont par exemple contribué à renforcer la capacité des forces de sécurité à mieux prévenir, prédire et lutter contre toute forme de crime.

C'est dans ce contexte d'informatisation qu'a lieu ce que certains experts nomment parfois la *«mise en données »* de la société :

« Bienvenue dans le futur. Là où tout ce qui vous concerne est sauvegardé. Un futur où vos actions sont enregistrées, vos mouvements surveillés, et où vos conversations ne sont plus éphémères. Un futur qui n'est pas né d'une contre-utopie à la '1984', mais de la tendance naturelle des ordinateurs à produire des données. »

Cette éloquente citation[3] du spécialiste en sécurité informatique Bruce Schneier[4] pose la question de la vie privée à l'ère numérique. Il est en effet extrêmement difficile pour un individu de garder le contrôle sur ses données personnelles puisque celles-ci dépendent d'une multitude d'infrastructures différentes et sont souvent stockées sur de lointains serveurs. La mise en données de la société pose également le problème du consentement éclairé : en réalité, seules environ 20% des données collectées sont prélevées avec l'autorisation de l'utilisateur. L'internet des objets (objets communicants) rend le contrôle de l'individu sur ses données d'autant plus difficile qu'il n'est souvent pas conscient de la quantité de données qu'il génère, ni du chemin qu'elles parcourent. Enfin, les NTIC permettent de surveiller les individus grâce aux données personnelles laissées en ligne, mais aussi en «repersonnalisant» des données qui ne sont pas personnelles à la base. Par exemple, à partir des données laissées par les utilisateurs sur les réseaux sociaux, il est possible de dresser des profils individuels assez complets en procédant à des recoupements.

Ces évolutions technologiques ont donné naissance à une forme de capitalisme numérique, basé sur l'exploitation des données. Celles-ci font

3. Traduction libre. Pour l'original voir : Bruce Schneier : Privacy in the Age of Persistence. (2009) https://www.schneier.com/blog/archives/2009/02/privacy_in_the.html
4. Bruce Schneier est un spécialiste de renommée mondiale en cryptologie et en sécurité informatique. Il est le fondateur de la société Counterpane Internet Security

l'objet d'une large exploitation commerciale par les plateformes internet, pas toujours consentie. Sans nécessairement en avoir conscience, l'individu laisse de nombreuses traces le concernant sur internet, et en particulier sur les réseaux sociaux (ex : informations sur ses loisirs et ses goûts, photos personnelles). Celles-ci possèdent une valeur inestimable pour les entreprises du secteur privé cherchant à développer des profils de consommateurs. Alors que certains s'inquiètent de cette monétisation des données personnelles, d'autres suggèrent d'entériner cet état de fait en créant un droit de propriété sur les données personnelles, afin que les individus puissent les commercialiser et en tirer un revenu.

Les défis sécuritaires émergeant de la «mise en données » de la société

Si l'informatisation des sociétés est souvent synonyme de progrès, elle génère toutefois certains risques pour les individus, les économies et les Etats. La cybercriminalité, c'est-à-dire l'ensemble des infractions susceptibles d'être commises ou facilitées par l'utilisation d'un système informatique, généralement connecté à un réseau, comprend deux groupes :

- Les infractions liées aux systèmes d'information et aux systèmes de traitement automatisé des données: l'accès et l'utilisation frauduleuse de données, l'altération de systèmes informatiques, les cyber-attaques, etc.

- Les infractions liées aux formes de criminalité dite traditionnelles: l'utilisation des NTIC par les organisa-tions criminelles ou terroristes pour fa¬ciliter leurs activités, les escroqueries (usage frauduleux de cartes de crédit en ligne, phishing), les menaces et inju¬res diffusées via les nouveaux moyens de communication électronique, la contrefaçon, la diffusion d'images pé-dopornographiques, la diffusion de méthodes permettant la réalisation de crimes et délits, etc.

Cette nouvelle forme de cybercriminalité pose des risques pour la souveraineté nationale. Le cyberespace ne connaît pas de frontières géographiques : les cyberattaques peuvent toucher les infrastructures civile et militaire des Etats. Afin de relever ce nouveau défi, le sommet de l'OTAN de septembre 2014 a reconnu les cyberattaques massives comme acte de guerre auquel il peut être répondu militairement[5].

Plus spécifiquement, la question de la protection des données personnelles s'adresse en premier lieu au citoyen. Ce dernier peut non seulement être victime de la criminalité liée aux NTIC, mais également devoir affronter des risques liés à la collecte et au traitement abusif de ses données personnelles par les secteurs privés et publics. De nombreuses données personnelles sont collectées et stockées par exemple par l'Etat, les services de sécurité, les banques, ou encore les assurances. Souvent le citoyen ne sait pas réellement comment sont stockées ses données, ni pour combien de temps et dans quel but. Cet état de fait pose notamment la question du consentement non-éclairé et de la perte de contrôle de l'individu sur ses propres données. Il existe également un risque en lien avec certaines données personnelles **sensibles** (religion, opinions politiques, maladies, orientations sexuelles) dont la divulgation pourrait avoir un impact direct sur la vie de la personne concernée et compromettre ses droits et libertés fondamentales.

5. http://www.nato.int/cps/en/natohq/official_texts_112964.htm

Le difficile équilibre entre impératifs sécuritaires et respect des droits humains

Pour faire face aux menaces, les Etats ont souvent recours à des mesures renforçant le pouvoir des services de sécurité de collecter, traiter et stocker certaines données à caractère personnel. En 2015, dans le cadre de la lutte anti-terroriste, la France a par exemple adopté une nouvelle loi sur le renseignement visant à définir le cadre dans lequel les services de renseignement sont autorisés à collecter et conserver des données (Voir encadré page 9). Cette loi autorise par exemple la mise en place de boîtes noires et d'IMSI Catcher[6] auprès des opérateurs de télécommunications. Cette mesure est sujette à controverse puisqu'elle implique la surveillance non seulement des suspects, mais également des non-suspects.

Sur une note similaire, l'Australie a adopté la même année une loi qui autorise 24 agences à avoir accès sans mandat judiciaire aux données personnelles. La seule condition à remplir est de tenir un registre secret des personnes concernées. Cette loi établit un champ d'action relativement vaste : les services de sécurité peuvent avoir accès à toutes les activités de courrier électronique, de téléphonie fixe et mobile, ainsi qu'aux activités en ligne et sur les réseaux sociaux par les utilisateurs.

La Suisse a également voté à large majorité une loi autorisant la surveillance de toutes les communications, ainsi que l'envoi de chevaux de Troie pour espionner les ordinateurs à distance. Cette loi a été dénoncée comme irrespectueuse des droits fondamentaux. Elle est également critiquée car au lieu d'investir dans la sécurité informatique, l'État peut utiliser les mêmes failles que celles dont abusent les criminels.

Si les besoins sécuritaires sont compréhensibles, ces lois sont souvent dénoncées comme trop intrusives. Elles tendent à mettre à mal le droit des citoyens à la protection de leur vie privée, et peuvent affecter indirectement d'autres droits et libertés fondamentales (ex: liberté d'opinion, d'expression, de conscience, etc.). Certaines données sont sensibles et peuvent faire l'objet d'un détournement malencontreux, voire même dangereux pour l'individu concerné. À titre d'exemple, l'Allemagne, profondément marquée par son histoire, a connu un développement du droit à la vie privée unique en Europe en reconnaissant en 1983 un droit fondamental à « l'autodétermination informationnelle» (voir encadré page 11).

Pour résumer, le lien entre protection des données personnelles et bonne gouvernance du secteur de la sécurité est double. D'une part, l'Etat a pour rôle de garantir la sécurité de ses citoyens, face à la criminalité liée aux NTIC, comprenant les infractions portant atteinte aux données personnelles et à la vie privée. Selon la même logique, il doit également garantir la sécurité de ses infrastructures et de son économie.

D'autre part, en luttant contre les menaces par la mise en place de politiques de surveillance, l'Etat compromet certains droits et libertés fondamentales de ses citoyens, dont notamment le droit à la protection de la vie privée. Il convient donc de s'interroger sur la façon de garantir l'équilibre entre impératifs sécuritaires et respect des droits et libertés fondamentales, de manière générale et en cas de crise ou de menace également.

6. Un IMSI-catcher (International Mobile Subscriber Identity) est un matériel d'espionnage téléphonique utilisé pour l'interception du trafic de téléphonie mobile et pour pister les mouvements des terminaux et donc de leurs porteurs.

LUTTE ANTITERRORISTE ET PROTECTION DES DONNÉES PERSONNELLES : LE CAS FRANÇAIS

En France, la loi relative au renseignement a été adoptée le 24 juillet 2015 sur fond de lutte antiterroriste. Cette nouvelle loi :

- vise à définir le cadre dans lequel les services de renseignement sont autorisés à collecter et conserver des données.
- permet aux services de renseignement de recourir à certaines techniques de collecte d'informations permises à l'origine uniquement dans un cadre judiciaire.
- permet le recours à certaines techniques considérées comme fortement intrusives (boîtes noires, IMSI catcher).
- réaffirme le respect de la vie privée dans toutes ses composantes, y compris l'inviolabilité du domicile, le secret des correspondances le respect des données personnelles.
- permet à l'autorité publique de porter atteinte à la vie privée en cas de « menaces, de risques et d'enjeux liés aux intérêts fondamentaux de la Nation », dont notamment la sécurité nationale et la prévention du terrorisme.
- institue la Commission nationale de contrôle des techniques de renseignement* (CNCTR) en tant que nouvelle autorité administrative indépendante chargée de valider les motifs invoqués pour certaines écoutes administratives.
- soumet la mise en œuvre des techniques de renseignement à une autorisation du Premier ministre, après avis non contraignant de la CNCTR.
- ne concerne pas les professions soumises au secret professionnel, lesquelles ne peuvent faire l'objet d'une surveillance administrative sauf avis contraire de la CNCTR.

La Commission Nationale de l'Informatique et des Libertés, ainsi qu'une frange de la société civile et de la classe politique ont dénoncé le caractère vague de certaines dispositions et le manque de contre-pouvoirs (restriction du contrôle judiciaire).

**La CNCTR est composée de deux députés, deux sénateurs, deux magistrats, deux membres du Conseil d'Etat et un expert en matière de communications électroniques.*

2. Protéger les données personnelles à l'ère numérique

Dans le cadre d'une politique de protection des données personnelles, l'établissement d'un équilibre entre impératifs sécuritaires et respect des droits et libertés fondamentaux dépend largement de la mise en place d'un cadre juridique clair, ainsi que de mécanismes de contrôle efficaces.

Légiférer au niveau national et international

Les premières lois sur la protection des données personnelles sont apparues dans les années 1980. À l'époque, les gros systèmes informatiques étaient rares et la possibilité de traiter les données personnelles n'existait pas encore. Les problèmes posés par la surveillance de masse sont survenus plus tard et ont nécessité la mise en place d'un cadre juridique, lequel n'a cessé d'évoluer depuis.

Les différentes approches en matière de protection des données personnelles peuvent être classifiées en fonction de l'importance qu'elles donnent au citoyen (ici par ordre d'importance croissant) :

- Lutte contre le traitement abusif de données: l'individu peut porter plainte si ses données ne sont pas collectées, traitées, utilisées dans le respect de la loi.
- Autodétermination individuelle: l'individu a la maîtrise de ses données.
- Droit de propriété: l'individu reste propriétaire de ses données (Cour constitutionnelle allemande).

Différents types de loi et de règlementations permettent de concrétiser ces approches sur le plan juridique :

- Les lois générales: les lois générales incluent les principes clés relatifs à la protection des données personnelles (voir encadré ci-dessous). Ces lois sont parfois vagues et la jurisprudence joue donc un rôle essentiel.
- Les règlementations sectorielles: ce sont des règlementations spécifiques applicables pour certains domaines précis (télécommunications, secteur bancaire, secteur de la santé).
- Les décisions cadres prises par les autorités de contrôle: ces textes juridiques diffèrent selon les contextes nationaux ; la protection de la vie privée ne revêtant pas la même importance selon les pays. Par exemple, le cadre juridique en matière de protection des données personnelles à Singapour est moins strict que dans la plupart des pays européens.

Principes clés du droit à la protection des données personnelles

- Droit à l'oubli et droit au déréférencement: Il permet à un individu de demander que certaines données personnelles qui pourraient lui nuire ne soient plus traitées. Ce droit s'applique soit par le retrait de ces données des sites où elles apparaissent (droit à l'effacement), soit par un déréférencement du site par les moteurs de recherches (droit au déréférencement).
- Droit d'accès à l'information: chaque individu est en droit de savoir si des données le concernant sont traitées et si oui comment et à quel but.
- Droit de blocage, droit de suppression et de modification: chaque individu est en droit bloquer, supprimer et modifier les données le concernant qui sont collectées et traitées.
- Principe de «bonne foi»: la personne en charge du traitement des données doit le faire de manière transparente et ouverte. Ce principe pose problème pour le secteur de la sécurité qui opère souvent dans des contextes de confidentialité et de secret.

- Principe de non réutilisation des données: les données traitées dans un but précis ne peuvent être réutilisées dans un autre but.

Au niveau européen, les principaux instruments permettant de garantir le droit des individus à la protection des données personnelles et de lutter contre la cybercriminalité sont :

- La Convention Européenne des Droits de l'Homme de 1950 (CEDH): l'article 8 de la CEDH, proclame le droit de toute personne au respect «de sa vie privée et familiale, de son domicile et de sa correspondance». Ce principe s'applique aussi au secteur de la sécurité, tant pour les services de police que de renseignement. Toutefois, certaines restrictions de ce droit sont possibles dans le domaine de la sécurité à trois conditions cumulatives:
  a. l'ingérence doit être prévue par la loi, de manière suffisamment claire et précise afin que les individus puissent savoir à quoi s'attendre de la part des autorités;
  b. l'ingérence doit être strictement nécessaire dans une société démocratique (critère de proportionnalité) ;
  c. l'ingérence doit viser un intérêt légitime comme la sécurité nationale, la sûreté publique, ou la défense de l'ordre et à la prévention des infractions pénales.

- La Convention 108 du Conseil de l'Europe[7]: il s'agit du premier texte contraignant pour la protection des données personnelles. Elle a été ouverte à signature en 1981 et reste aujourd'hui, le seul acte international à force juridique obligatoire dans le domaine de la protection des données. La Convention 108 vise à protéger les droits et libertés fondamentales de toute personne physique, notamment le droit au respect de la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant. Elle est basée sur l'article 8 de la CEDHD, précédemment cité. Pour plus de détails, voir le tableau page XX.

- La Recommandation R(87)15 du Conseil de l'Europe, adoptée en 1994, règlemente l'utilisation de données personnelles dans le secteur de la police. Elle va encore plus loin que «la Convention 108» pour la protection des données personnelles dites sensibles.

- La Convention de Budapest du Conseil de l'Europe contre la cybercriminalité: il s'agit du premier traité international sur les infractions pénales commises via l'Internet et d'autres réseaux informatiques. Comme le précise son préambule, la Convention de Budapest a pour principal objectif de poursuivre «une politique pénale commune destinée à protéger la société contre la criminalité informatique, notamment par l'adoption d'une législation appropriée et la stimulation de la coopération internationale». Le texte a été ouvert à signature le 23 novembre 2001 à Budapest et est entré en vigueur en 2004.

Il est important de souligner que, dans l'esprit du Conseil de l'Europe, la protection des données n'a pas pour objectif d'empêcher le traitement légitime de données personnelles ni d'entraver le travail des autorités policières et judiciaires. Elle fixe simplement un cadre à respecter pour garantir le respect des droits et des libertés fondamentales et notamment le droit à la vie privée. La Convention 108 et la Convention de Budapest visent donc à mettre en place des limitations et des sauvegardes afin d'assurer que les interventions et pouvoirs des autorités policières et judiciaires restent proportionnels.

7. Voir présentation de la Convention page 13.

POINTS CLÉS DE LA CONVENTION 108 DU CONSEIL DE L'EUROPE

Article	Explication
Préambule et article 1	Objectifs de la Convention 108 : protéger les droits et libertés fondamentales de toute personne physique, notamment le droit au respect de la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant
Article 3	Champ d'application : tout traitement de données à caractère personnel dans les secteurs privé et public, y compris ceux effectués par les autorités judiciaires ou celles chargées de l'application de la loi.
Article 4	Chaque Partie à la Convention prend, dans son droit interne, les mesures nécessaires pour donner effet aux principes de base pour la protection des données énoncés dans la Convention.
Article 5	Qualité des données : Les données à caractère personnel faisant l'objet d'un traitement automatisé sont: a. obtenues et traitées loyalement et licitement ; b. enregistrées pour des finalités déterminées et légitimes et ne sont pas utilisées de manière incompatible avec ces finalités ; c. adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées ; d. exactes et si nécessaire mises à jour ; e. conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées.
Article 6	Interdiction, en l'absence de garanties juridiques convenables, de traiter les données «sensibles», telles que l'origine raciale, l'opinion politique, l'état de santé, les convictions religieuses, la vie sexuelle ou les condamnations pénales d'une personne.
Article 8	Garanties pour la personne concernée par le traitement de ses données personnelles: a. connaître l'existence d'un fichier automatisé de données à caractère personnel, ses finalités principales, ainsi que l'identité et la résidence habituelle ou le principal établissement du maître du fichier; b. obtenir à des intervalles raisonnables et sans délais ou frais excessifs la confirmation de l'existence ou non dans le fichier automatisé, de données à caractère personnel la concernant ainsi que la communication de ces données sous une forme intelligible; c. obtenir, le cas échéant, la rectification de ces données ou leur effacement lorsqu'elles ont été traitées en violation des dispositions du droit interne donnant effet aux principes de base énoncés dans les articles 5 et 6 de la présente Convention;

d. disposer d'un recours s'il n'est pas donné suite à une demande de confirmation ou, le cas échéant, de communication, de rectification ou d'effacement, visée aux paragraphes b et c du présent article.

Article 9	Il est possible de déroger aux dispositions des articles 5, 6 et 8 de la présente Convention lorsqu'une telle dérogation, prévue par la loi de la Partie, constitue une mesure nécessaire dans une société démocratique: a. la protection de la sécurité de l'Etat, à la sûreté publique, aux intérêts monétaires de l'Etat ou à la répression des infractions pénales; b. la protection de la personne concernée et des droits et libertés d'autrui.

Mettre en place des mécanismes de contrôle

Si l'existence d'une législation précise et adéquate est primordiale pour protéger les données personnelles des citoyens, celle-ci doit être accompagnée de mécanismes visant à contrôler la bonne application des lois. Tout d'abord, des mécanismes judiciaires de contrôle sont indispensables. Dans le cadre du secteur de la sécurité, les normes et bonnes pratiques internationales exigent que les interceptions judiciaires (voir encadré ci-contre) ne soient possibles que dans le cadre d'une instruction et avec l'aval d'un magistrat, et ce, afin d'éviter que les services de police n'abusent des méthodes intrusives (ex: écoutes téléphoniques). La justice a également pour mission d'appliquer les sanctions prévues par la loi en cas de violation avérée des principes de protection des données personnelles. Il est également nécessaire de donner le droit à des réparations aux citoyens en cas de traitement abusif de leurs données personnelles.

INTERCEPTIONS JUDICIAIRES ET INTERCEPTIONS ADMINISTRATIVES : QUELLE DIFFÉRENCE ?

La législation nationale de nombreux pays établit une distinction entre interceptions judiciaires et interceptions administratives.

Les interceptions judiciaires se justifient par les besoins d'une enquête et sont donc réalisées dans le cadre d'une instruction judiciaire. Dans ce cas, la police nécessite l'autorisation d'un magistrat (ex : juge d'instruction, procureur selon les contextes nationaux) pour recourir à l'interception de télécommunications.

Les interceptions administratives font référence aux intrusions des services de police ou de renseignement dans les communications privées dans l'objectif d'anticiper un grave danger à la sécurité nationale ou aux intérêts fondamentaux de l'Etat (ex : terrorisme, grand banditisme, espionnage économique). Le cadre légal selon lequel ces interceptions sont permises et réglementées diffère largement d'un pays à l'autre, avec différents degrés de permissivité. Ce type d'interceptions est source de nombreuses inquiétudes en raison du manque de mécanismes de contrôle qui les caractérise généralement. Certains citoyens y voient notamment des risques de surveillance de masse et d'atteinte à leur vie privée.

En outre, l'un des mécanismes institutionnels de contrôle les plus répandus consiste à mettre en place une autorité nationale indépendante chargée du contrôle de la protection des données personnelles. Conformément au Protocole additionnel à la Convention 108 du Conseil de l'Europe, cette autorité doit être dotée des missions suivantes :

- Investigation: l'autorité doit pouvoir demander et obtenir des informations concernant les traitements des données personnelles.
- Intervention: l'autorité doit par exemple pouvoir obliger le responsable du traitement à rectifier des données incorrectes ou collectées de manière illégales, les effacer ou les détruire.
- L'autorité doit avoir le pouvoir soit d'ester en justice, soit de porter à la connaissance de la justice toute violation aux principes de la protection des données personnelles.
- Traitement des plaintes: l'autorité doit pouvoir traiter les plaintes des personnes relatives à la protection de leurs droits et libertés à l'égard du traitement des données personnelles.

Les pouvoirs des autorités nationales de contrôle de la protection des données personnelles sont plus ou moins larges selon les pays[8]. Dans certains Etats fédéraux, une instance au niveau national se partage les prérogatives de contrôle de la protection des données personnelles avec des instances au niveau régional. C'est notamment le cas en Allemagne (voir encadré page 15).

Les mécanismes de démocratie directe peuvent également permettre de renforcer le contrôle de la protection des données personnelles. En Suisse, suite à l'adoption de la nouvelle loi sur le renseignement jugée trop intrusive par certains citoyens, une collecte de signatures a débouché sur l'introduction d'un référendum national qui aura lieu durant l'année 2016[9].

Finalement, il y aurait également besoin de mécanismes internationaux de contrôle, mais – malgré les discussions sur le sujet, les participants au séminaire des 19 et 20 octobre considèrent que cela paraît utopique pour le moment.

8. Voir: European Union Agency for Fundamental Rights : Data Protection in the European Union : the role of National Data Protection Authorities - Strengthening the fundamental rights architecture in the EU II, 2010.
   Voir aussi: DLA Piper - Data Protection Laws of the World
   http://www.dlapiperdataprotection.com/#handbook/enforcement-section/c1_CH
9. Plus d'informations disponibles sur le site du groupement de la société civile contre la loi sur le renseignement : https://www.lrens.ch/

FÉDÉRALISME ET PROTECTION DES DONNÉES PERSONNELLES : LE CAS DE L'ALLEMAGNE

L'Allemagne est un Etat fédéral régi selon les principes de subsidiarité et de séparation verticale des pouvoirs*. De ce fait, la protection des données personnelles fait l'objet d'une réglementation différenciée au niveau du Bund *(Etat fédéral)* et des seize Länder *(Etats fédérés)*. Les administrations du Bund et des Länder sont soumises au principe de séparation informationnelle**.

	Bund	**Länder**
Cadre légal	- Loi fédérale sur la protection des données personnelles (DP) - Règlementations sectorielles (ex: loi sur les télécommunications)	- Lois des *Länder* relatives à la protection des DP - Règlementations sectorielles (ex : lois régionales sur la police)
Champ d'application	- Administrations du *Bund* - Prestataires privés et publics de services postaux et/ou de télécommunications	- Administrations des *Länder* et des communes - Secteur privé (sauf prestataires de services postaux et/ou de télécommunications)
Institutions indépendantes de contrôle	Un Commissaire fédéral pour la protection des DP et la liberté de l'information	16 Commissaires régionaux pour la protection des DP et la liberté de l'information
Acteurs du secteur de la sécurité concernés (liste non-exhaustive)	- Parlement fédéral - Ministères fédéraux de l'Intérieur, de la Défense, de la Justice - Office fédéral de police criminelle - Police fédérale - Services fédéraux de renseignement - Office fédéral de Protection de la Constitution (renseignement)	- Parlement régionaux - Ministères régionaux de l'Intérieur, de la Défense, de la Justice - Services de police - Offices régionaux de Protection de la Constitution (renseignement) - Entreprises privés de sécurité (ex: Securitas)

Conséquences pour la gouvernance du secteur de la sécurité:

- Le manque d'harmonisation des lois ne garantit pas la même protection contre les mesures de surveillance intrusives de la police d'un *Land* à un autre.
- Une protection efficace des données personnelles nécessite un effort constant de coordination et de législation entre les *Länder*, le *Bund*, et le niveau européen. Par exemple, les bases de données nationales communes aux services de police fédérale et régionales sont régulièrement critiquées du point de vue du droit de la protection des données personnelles.
- La création de bases de données nationales communes aux services de police et de renseignement – par exemple dans le cadre de la lutte antiterroriste – est controversée en raison du principe de séparation informationnelle.

** Selon le principe de subsidiarité, la responsabilité d'une action publique, lorsqu'elle est nécessaire, doit être allouée à la plus petite entité capable de l'endosser. Le principe de répartition verticale des pouvoirs fait référence à la répartition des compétences entre l'Etat fédéral et les Etats fédérés qui le composent.*

*** L'échange de données à caractère personnel entre deux administrations publiques ne peut avoir lieu que si une loi le permet. Ce principe permet d'éviter un échange et une centralisation non-nécessaires de données.*

Prendre en compte les approches judiciaire, technologique, managériale et citoyenne

Une approche purement législative de la protection des données personnelle présente certaines limites telles que :

- l'impossible consentement éclairé des utilisateurs,
- le comportement parfois irresponsable des acteurs qui traitent, captent, croisent, échangent, vendent les données,
- la nécessité mais l'impossibilité de légiférer au niveau mondial,
- la difficulté de la mise en place de contrôle tant au niveau national qu'international.

De ce fait, cette approche doit être complétée par d'autres solutions. L'approche judiciaire et administrative apporte certains éléments de réponse: elle permet notamment de dénoncer les cas d'abus de collecte et d'utilisation des données personnelles et les incivilités ou infractions commises via leur utilisation. Une augmentation des dénonciations constituerait un signal fort pour les politiques pour débloquer plus de moyens de sécurisation. Toutefois, la majorité des victimes de ces abus ne les dénonce pas. En Suisse, on tend à ne rien faire car on ne voit pas encore la nécessité.

L'approche technologique apporte certaines réponses:

- l'affinement des algorithmes,
- la cryptographie (solution de chiffrement),
- la gestion des systèmes et des utilisateurs,
- la gestion des accès,
- la gestion des identités numériques.

Néanmoins, la plupart des internautes n'utilisent pas de solution de chiffrement / de cryptographie. De plus, le chiffrement ne sert à rien pour les risques de chantages, de dénonciations ou encore de chantage économique. Enfin, en attendant que les algorithmes s'améliorent, il est nécessaire d'adapter les mesures de protection, non pas

en légiférant à posteriori sur l'évolution des plateformes numériques, mais en comprenant, anticipant et si possible, en agissant sur l'évolution des plateformes numériques.

L'approche managériale doit également être renforcée dans l'objectif d'une :

- meilleure gestion des systèmes d'information et de leur sécurité,
- mise en place renforcée de mesures préventives et réactives,
- mise en place renforcée d'audit de sécurité, si possible obligatoire (attention toutefois à ce que les mécanismes d'audit ne portent pas atteinte à la protection des données personnelles).

Enfin, l'approche citoyenne doit faire partie intégrante de la politique de protection des données personnelles. Il est ainsi primordial de :

- Prendre conscience de ce qu'est la vie privée et des problèmes pouvant résulter de sa violation.
- Sensibiliser et éduquer les individus dès le plus jeune âge à des pratiques numériques cohérentes (ex : peut-être à travers les cursus scolaires).
- Développer plus d'associations dédiées à la protection des données personnelles.
- Exiger des garanties raisonnables de respect des droits fondamentaux.
- Communiquer les besoins, les problèmes des utilisateurs et les faire remonter vers les autorités publiques.

Se poser les bonnes questions

Lors du séminaire des 19 et 20 octobre 2015, certains participants ont souligné que la question du contrôle des surveillants n'est posée que de façon partielle. L'attention se porte généralement sur l'Etat en tant que grand surveillant, mais en réalité, il existe une multitude de petits surveillants qui détiennent un important réservoir d'informations à caractère personnel : les assurances, les péages autoroutiers, les services de taxi, les plateformes de santé, les fournisseurs d'énergie, les compagnies aériennes, les consortiums de cartes de crédit, les réseaux sociaux, etc. Sans toujours s'en rendre compte, le citoyen bénéficie de services en échanges de données.

En outre, si l'Etat a un rôle important à jouer en tant que législateur et régulateur, seule une approche participative permettra d'obtenir des résultats optimaux. Les institutions publiques, le secteur privé, la société civile sont tous concernés par la problématique de protection des données personnelles et, pour cette raison, doivent travailler ensemble à des solutions.

Enfin, on ne peut pas penser à la protection des données des citoyens, sans faire également référence à la protection des données de l'Etat et de l'économie. Il faut donc en priorité s'intéresser au mode de gouvernance de l'Etat et en protéger les infrastructures (numérique ou non) pour finalement avoir un levier de protection des droits humains. Si l'Etat protège ses institutions de manière efficace dans ce contexte de données, il pourra alors mieux protéger les données de ses citoyens.

3. Garantir le droit d'accès à l'information en tant que pilier majeur de la protection des données personnelles

Comme déjà évoqué précédemment, le droit d'accès à l'information constitue l'un des principes clés du droit à la protection des données personnelles. La transparence renforce la confiance des citoyens dans les autorités publiques.

Ce droit d'accès à l'information peut être défini juridiquement par le :

- Droit d'accès commun: il s'agit du droit posé par les lois sur l'information. Le citoyen est en droit de savoir ce que fait l'Etat et ce dernier est tenu d'agir avec transparence.
- Droit d'accès individualisé: il règlemente l'accès aux données individuelles, ce que l'on en fait et dans quel but.

Dans les deux cas, les normes et standards internationaux préconisent deux modalités d'exercice du droit d'accès à l'information, la gratuité de la procédure d'accès, ainsi que la garantie de rapidité. De plus, des mécanismes de contrôle de l'application de ce droit doivent être mis en place, comme par exemple des autorités de contrôle. Dans certains pays (Suisse, Hongrie), une seule et même autorité est responsable du contrôle de l'application du droit d'accès à l'information et de la protection des données. Les avis divergent sur la pertinence de ce double mandat.

L'une des principales difficultés de la règlementation du droit d'accès à l'information consiste à définir le régime des exceptions à ce droit. Dans de nombreux cas, les législations nationales disposent de clauses générales permettant de refuser l'accès à certaines informations, notamment dans le cadre des activités de sécurité et de défense, ou bien lorsque les informations demandées concernent la vie privée d'autrui. La question se pose toutefois de savoir si ces exceptions doivent être intégrées dans la législation générale ou bien faire l'objet d'une législation spéciale. En outre, il est difficile d'adopter des clauses de secret plus détaillées. Enfin, le caractère excessivement étendu et flou des exceptions au droit d'accès laisse la porte ouverte à des activités illégales et des utilisations abusives.

Les *Principes de Tshwane sur la sécurité nationale et le droit à l'information (2013)* peuvent apporter des éléments de réponses pour trouver le juste équilibre. Ces principes définissent un certain nombre d'éléments permettant d'établir un équilibre entre le secret officiel et le droit de savoir du public. Ils sont issus d'une consultation internationale conduite pendant plus de deux ans par l'*Open Society* Justice Initiative et à laquelle ont participé des gouvernements, d'anciens responsables de la sécurité, des groupes de la société civile et des universitaires.

Les *Principes de Tshwane* précisent notamment que:

- Les informations doivent être maintenues secrètes seulement si leur divulgation présente « un risque réel et identifiable de nuisance grave à un intérêt légitime de sécurité nationale ». (Principe 3)
- Les informations relatives à de graves violations des droits humains internationaux ou du droit humanitaire doivent toujours être divulguées. (Principe 10A)
- Le public doit avoir accès aux informations relatives aux programmes de surveillance. (Principe 10E)
- Aucune entité gouvernementale ne doit être

catégoriquement exemptée d'exigences de divulgation. (Principe 5)

- Les représentants de l'État qui agissent dans l'intérêt du public en exposant des abus du gouvernement doivent être protégés contre toute mesure de représailles. (Principe 40)

Les *Principes de Tshwane* reconnaissent également le caractère secret des :

- plans d'engagement des forces armées,
- informations sur l'arsenal et les infrastructures de défense,
- mesures de protection des institutions étatiques et les ressources allouées à cet effet (ex : protections contre le sabotage),
- informations sur les modes opératoires des services secrets,
- informations transmises par des services étrangers sous le sceau du secret.

La vigilance est de mise: parfois, les autorités publiques invoquent d'autres raisons pour restreindre l'accès à l'information. C'est notamment le cas des clauses sur la protection de la vie privée d'autrui qui peuvent être détournées pour faire de la rétention d'information. Par exemple, les autorités américaines ont refusé de donner accès à la liste des noms et des pays d'origine des détenus de Guantanamo à l'agence de presse Reuters, sous prétexte qu'il fallait protéger la vie privée de ces derniers.

B. La protection des données personnelles dans le cadre du secteur de la sécurité au Maroc

Depuis le début du XXI[ème] siècle, le Maroc témoigne de sa volonté de respecter et de protéger les droits humains. Les recommandations de l'Instance Equité et Réconciliation représentent des acquis importants en la matière. Lors du séminaire des 19 et 20 octobre 2015, certains participants ont souligné que la nouvelle Constitution de 2011 avait posé un nouveau cadre de référence ambitieux et généré une forme «d'attente» d'institutionnalisation du principe de bonne gouvernance.

1. Cadre juridique et institutionnel

Aperçu du cadre juridique national

Dans le cadre des réformes en cours depuis le début des années 2000, le Royaume tente de trouver le juste équilibre entre impératifs sécuritaires et droit à la protection de la vie privée. De ce fait, la protection des données personnelles constitue un chantier en plein essor. Plusieurs textes nationaux vont dans ce sens, dont notamment (par ordre d'importance juridique) :

- l'article 24 de la Constitution de 2011 consacrant le droit à la protection de la vie privée,
- la loi 09-08 sur la protection des données personnelles,
- le Dahir relatif à l'échange des données électroniques,
- la stratégie nationale pour la société de l'information, dite « Maroc numérique 2013 » : elle inclut une mise à jour du cadre législatif, des activités de sensibilisation du public sur les dangers de la criminalité liée aux nouvelles technologies et la mise en place de la Direction Générale de la sécurité des systèmes d'informations (créée en 2011),
- la charte de nommage.

La loi 09-08 relative à la protection des individus à l'égard du traitement des données à caractère personnel

À l'origine, cette loi générale a été adoptée afin de protéger les personnes de l'utilisation abusive des données personnelles, en premier lieu et de faciliter par ailleurs la délocalisation de certaines activités du secteur tertiaire de l'Europe vers le Maroc (ex : call center). Elle précise notamment que « l'informatique est au service du citoyen (...) elle ne doit pas porter atteinte aux droits de l'homme» (09-08). Elle inclut les piliers suivants :

- les droits des personnes physiques concernées par le traitement de leurs données personnelles,
- les obligations des responsables du traitement des données à caractère personnel,
- les exigences de confidentialité à remplir,
- la mise en place d'une autorité de contrôle indépendante,
- les sanctions en cas de violation de la loi 09-08.

Il est important de souligner ici que l'article 2 de la loi 09-08 exclut les données recueillies dans le

cadre des activités de défense et sécurité du champ d'application de la loi. Ceci n'est pas une exception en comparaison internationale. La question est à présent de savoir si l'article 24 de la Constitution pourrait éventuellement servir de base à la protection des données personnelles dans le cadre des activités de défense et de sécurité.

L'adhésion à des instruments internationaux de protection des données personnelles

Le Maroc est en voie d'adhésion à plusieurs conventions internationales dans le cadre de la politique de voisinage de l'Union Européenne, dont notamment la Convention de Budapest et la Convention 108 du Conseil de l'Europe et son Protocole additionnel. À noter que la Convention 108 du Conseil de l'Europe admet des restrictions – mais pas d'exceptions – aux principes fondamentaux de la protection des données personnelles pour des raisons relatives à « la protection de la sécurité de l'Etat, à la sûreté publique, aux intérêts monétaires de l'Etat ou à la répression des infractions pénales » (CoE, Convention 108, Art.9). L'article 2 de la loi 09-08 évoquée précédemment semble de fait contraire à cette disposition.

Le Maroc participe également au projet Action Globale sur la Cybercriminalité (GLACY) de l'Union européenne et du Conseil de l'Europe. Ce projet a pour objectif «de permettre aux autorités judiciaires pénales de s'engager dans la coopération internationale en matière de cybercriminalité et de preuve électronique sur le fondement de la Convention de Budapest sur la cybercriminalité.» Il s'agit entre autres de mobiliser les responsables politiques, harmoniser la législation, renforcer le partage d'information, la formation judiciaire, et les moyens des organes de répression.

La Commission nationale pour le contrôle de la protection des données personnelles (CNDP)

La CDNP a été instaurée par la loi 09-08 du 18 février 2009. Elle a pour prérogative générale de mettre en œuvre et de veiller au respect des dispositions de la loi 09-08 et des autres textes de références en matière de protection des données à caractère personnel. La CNDP est composée de:

- un président nommé par Sa Majesté le Roi,
- six membres, nommés également par Sa Majesté le Roi, suite à une proposition du Premier ministre (deux membres), du Président de la Chambre des représentants (deux membres), du président de la Chambre des conseillers (deux membres).

Les membres de la commission sont désignés pour une période de cinq ans, renouvelable une seule fois.

Plus précisément, les missions de la CNDP sont les suivantes:

Information et sensibilisation: La CNDP mène auprès des individus, des organismes et des institutions publiques et privées des activités de sensibilisation visant à renforcer la connaissance de leurs droits et obligations en matière de protection des données personnelles. Dans ce cadre, la CNDP a mis à disposition un portail électronique actualisé régulièrement, produit des brochures d'information, des spots pour la radio et la télévision, et une émission radio hebdomadaire. La CNDP accompagne également les acteurs concernés dans la mise en conformité de leurs procédures de traitement des données personnelles. La priorité est en général donnée aux secteurs qui traitent le plus de données personnelles (ex : télécommunications, banques, assurances, centres d'appel, sites de vente en ligne, santé).

Conseil et proposition: La CNDP a pour rôle de conseiller tous les acteurs publics actifs dans le domaine de la protection des données personnelles (gouvernement, parlement, administration). Elle peut donner son avis sur les projets de loi et de règlements, présenter au gouvernement des propositions de législation, ou encore aider à préparer la position du Maroc lors de négociations internationales en la matière.

Protection et traitement des plaintes: La CNDP a pour rôle de traiter les plaintes des citoyens relatives aux violations de leur droit à la protection des données personnelles. La majorité des plaintes est reliée à la publicité abusive, aux spams, vidéosurveillance, etc. Le nombre de plaintes traitées a significativement augmenté entre 2011 et 2015 : une plainte en 2011 contre 355 en 2015. La CNDP traite également les déclarations et les demandes d'autorisation des responsables du traitement des données personnelles. Elle peut par exemple autoriser la conservation des données au-delà de la durée prévue et délivrer l'autorisation de traiter certaines catégories de données considérées comme sensibles. Enfin, la CNDP tient le registre national de la protection des données personnelles. Ce dernier contient par exemple la liste les fichiers traités par les autorités publiques et les autorisations de traitement délivrées.

Contrôle et investigation: La CNDP dispose de pouvoirs d'investigation et d'enquête lui permettant de contrôler et de vérifier que les traitements des données personnelles sont effectués conformément à la loi. Dans ce but, les agents de la CNDP peuvent accéder directement à tous les éléments intervenant dans les processus de traitement (les données, les équipements, les locaux, les supports d'information, etc.). Ces contrôles peuvent aboutir à des sanctions administratives, pécuniaires ou pénales.

Veille juridique et technologique: La CNDP surveille, étudie et analyse les tendances et les mutations technologiques, économiques, juridiques et sociétales pouvant affecter la protection des données personnelles au Maroc.

La Direction Générale de la Sûreté nationale

La Direction Générale de la Sûreté Nationale (DGSN) a pris plusieurs mesures afin de lutter contre les crimes liés aux NTIC. Elle a notamment créé plusieurs structures au niveau central, dont le Service de lutte contre la criminalité liée aux Nouvelles Technologies ainsi que le Service de lutte contre la cybercriminalité, tous les deux liés à la Police Judiciaire. Au niveau décentralisé, 29 brigades spécialisées et 4 laboratoires régionaux ont été mis en place. Enfin, plusieurs avancées ont eu lieu en matière de ressources humaines et matérielles: la DGSN recrute de plus en plus de profils spécialisés en cybercriminalité et cyberdéfense et a renforcé son équipement afin que ce dernier soit adapté aux exigences de l'informatique légale[10].

Lors du séminaire des 19 et 20 octobre 2015, une représentante de la DGSN a fourni un aperçu des infractions les plus courantes au Maroc pouvant mettre à mal la protection des données personnelles des citoyens. Il s'agit notamment :

- des atteintes aux personnes (y compris menace et extorsion qui ont fortement augmenté depuis 2013),
- des fraudes bancaires,
- des attaques aux systèmes d'information (généralement du type déni-de-service).

10. Le terme « informatique légale » est une adaptation de l'anglais «digital forensics». Il fait référence à l'ensemble des connaissances et méthodes qui permettent, dans le cadre d'enquêtes judiciaires, de collecter, conserver et analyser des preuves issues de supports numériques (ordinateurs, smartphones).

La Direction Générale de la Sécurité des Systèmes d'Information

Créée en 2011, la Direction Générale de la Sécurité des Systèmes d'Information a pour mission de:

- coordonner entre les différents ministères pour l'élaboration de la stratégie nationale de la sécurité des systèmes d'information,
- proposer des normes et standards de sécurité et gérer les autorisations liées à l'utilisation des certificats électroniques,
- assister et conseiller les infrastructures publiques et privées à l'instauration de normes de sécurité des systèmes d'information,
- mettre en œuvre les audits de sécurité des institutions publiques,
- mettre en place un système de veille, d'interception et de réponse aux attaques sur les infrastructures informatiques du pays et coordonner la réponse aux incidents,
- assurer la veille technique en sécurité pour anticiper les attaques et proposer les améliorations adéquates,
- proposer des cycles de formations et de sensibilisation à la sécurité des systèmes au profit des employés des administrations et institutions publiques.

2. Défis et opportunités

Défis sur le plan juridique

Comme évoqué précédemment, le Maroc a adopté une loi sur la protection des données personnelles dans le but de mettre en conformité sa législation nationale avec ses engagements internationaux. Si les participants du séminaire ont salué cette initiative, ils ont néanmoins plaidé en faveur d'un renforcement de la loi 09-08, notamment en matière de sanctions et d'indépendance administrative et financière de la CNDP. Certains participants regrettent également que la loi 09-08 ne prévoie pas de mécanismes de participation de la société civile à travers le CNDH.

En outre, il convient de préciser qu'à ce jour seuls trois types de fichiers concernant des données à caractère personnel sont encadrés par la loi, à savoir :

- la carte nationale d'identité électronique instituée par la loi 35-06,
- la fiche anthropométrique créée en 1925,
- le casier judicaire.

D'après certains intervenants et afin de prévenir la collecte et le traitement abusifs de données à caractère par les autorités publiques ou des entités privées, il est nécessaire que la réglementation soit étendue à d'autres types de fichiers. Par exemple, l'intervention du législateur parait nécessaire pour combler le vide en matière de biométrie, de surveillance et de géo-localisation. A ce propos, et dans le cadre de ses compétences, la CNDP a émis trois délibérations :

- la délibération n°478-2013 portant sur les conditions nécessaire à l'utilisation des dispositifs biométriques pour le contrôle d'accès,
- la délibération n° 350-2013 du 31 Mai 2013 portant sur les conditions nécessaires à la mise en place d'un système de vidéosurveillance dans les lieux de travail et dans les lieux privés communs,
- la délibération n° 17-2014 portant sur l'utilisation de géo-localisation de véhicules utilisés par des employés.

Dans une même veine, de nombreux participants ont souligné le besoin d'adopter rapidement une loi sur le droit d'accès à l'information conforme aux normes et standards internationaux. En effet, les citoyens doivent pouvoir accéder aux informations qui sont collectées à leur sujet et les restrictions de ce droit doivent être définies avec clarté et précision. Certains ont dénoncé le projet de loi 31-13 relatif au droit d'accès à l'information actuellement discuté au Parlement, en raison notamment de formulations vagues élargissant le périmètre des exceptions et des interprétations plus restrictives du droit d'accès. Selon le projet actuel et en dépit des normes et bonnes pratiques internationales, les demandeurs seraient obligés d'indiquer le but de leur démarche et s'exposeraient à des sanctions pénales en cas d'usage de l'information fournie dans un but autre que celui spécifié.

De plus, si les interceptions judiciaires sont régies par le Code pénal et sont soumises à l'instruction du parquet, les interceptions administratives ne font quant à elles l'objet d'aucun cadre légal. Certains participants au séminaire craignent que ce vide juridique ne laisse la porte ouverte à certains abus sous couvert de protection de la sécurité nationale (ex: écoutes téléphoniques injustifiées). Ils laissent donc le soin au législateur de remédier à cette situation.

Enfin, plusieurs intervenants se sont prononcés en faveur d'une législation claire et précise du secret professionnel et de ses restrictions. Dans le cadre de leur métier, les avocats sont parfois mis dans la confidence de certaines informations sensibles pouvant concerner par exemple la sécurité de l'Etat. Il convient de se demander si l'avocat doit dénoncer son client ou bien respecter le secret professionnel afin de protéger ce dernier. Les médecins rencontrent des difficultés similaires étant donné que certaines informations à caractère personnel peuvent avoir un impact social. Par exemple, les patients séropositifs ne peuvent pas occuper certaines positions militaires ou civiles et se retrouvent marginalisées si l'information circule. Le dilemme est ainsi de protéger la société d'un côté, et le patient lui-même de l'autre.

Défis sur le plan institutionnel

Plusieurs participants au séminaire ont souligné la nécessité de renforcer la bonne gouvernance au sein des institutions, notamment de la CNDP. Tout d'abord, l'Instance devrait disposer de ressources financières et humaines suffisantes. La Commission dispose à ce jour de sept membres, mais cet effectif semble trop faible face à la charge de travail (ex : 17 membres dans les commissions françaises et tunisiennes de protection des données personnelles).

D'autres participants se sont exprimés en faveur de la non-duplication des mandats pour les membres de la CNDP afin de garantir leur plein investissement dans les activités de la CNDP. Cette dernière rencontre également plusieurs défis sur le plan organisationnel : elle doit apprendre rapidement un nouveau métier, suivre le rythme effréné des nouvelles technologies, tout en répondant professionnellement aux requêtes et en tentant d'inculquer une nouvelle culture aux citoyens.

Certains participants ont aussi exprimé leur souhait de voir la CNDP plus transparente et ouverte envers les citoyens. En effet, si cette dernière dispose d'une stratégie de sensibilisation (ex: rubriques radiodiffusées, conventions signées avec certains secteurs), ses activités de communication externe ont été insuffisantes en raison du manque de ressources humaines et financières auquel elle fait face. Il s'agit donc

de remédier à ces manques afin de renforcer la visibilité de la CNDP. Les citoyens devraient par exemple mieux comprendre le cadre dans lequel elle opère (champ d'application de la loi) et la procédure pour recourir à ses services (déposer une plainte, demander un conseil, etc.).

Défis relatifs à l'application de la Convention 108 et de la Convention de Budapest du Conseil de l'Europe

La mise en œuvre de la Convention 108 du Conseil de l'Europe et de son Protocole additionnel au Maroc va nécessiter plusieurs réformes juridiques et institutionnelles. Tout d'abord et comme déjà évoqué auparavant, la loi 09-08 exclut les données recueillies dans le cadre des activités de défense et de sécurité de son champ d'application. La loi devra donc être modifiée pour être conforme à la Convention 108. De plus, le Maroc a entamé le processus d'adhésion à la Convention de Budapest. Avant de pouvoir la ratifier, le Royaume doit achever la mise en place de l'Unité d'enquête spécialisée et procéder à certains amendements législatifs, notamment dans le Code de Procédure Pénale.

Sur le plan opérationnel, la mise en œuvre des deux Conventions nécessite de mettre en place des garde-fous afin d'assurer que les interventions et pouvoirs des autorités policières et judiciaires respectent le principe de proportionnalité (gradation des mesures). Il s'agira également de renforcer :

- les moyens humains et financiers mis à disposition dans ce domaine,
- la coopération entre les différents services de sécurité,
- la formation des policiers, notamment pour l'enregistrement des plaintes relatives à la protection des données personnelles,
- la formation judiciaire,
- les partenariats publics-privés (ex : conditions de conservation des données par le secteur privé, modalités d'accès à ces données),
- la protection des enfants et des groupes à risques (minorités ethniques, religieuses).

Opportunités liées au renforcement de la protection des données personnelles

D'après les participants au séminaire, les services de sécurité font preuve d'une certaine ouverture d'esprit au sujet de la protection des données personnelles depuis le début des années 2000, et surtout depuis les réformes de 2011. L'idéal serait donc de saisir cette occasion afin d'engager une réflexion avec toutes les parties concernées sur la manière de protéger au mieux les données personnelles dans le cadre du secteur de la sécurité. Dans ce cadre, la réalisation d'une évaluation complète des structures du secteur de la sécurité impliquées dans le traitement des données personnelles pourrait être discutée (sont-elles efficaces ? Efficientes ? Ont-elles assez de ressources ?). Il serait également nécessaire de développer une vision stratégique commune à tous les acteurs concernés en matière de protection des données personnelles dans le cadre des activités de sécurité et de défense.

En outre, les discussions autour du renforcement de la protection des données personnelles devraient être complétées par un volet spécial sur les réseaux sociaux. Afin que le Maroc puisse établir une stratégie de protection des citoyens sur ces réseaux, il faudrait tout d'abord parler des risques et des menaces, les évaluer et sensibiliser le public à ce propos. Les citoyens ne sont pas toujours conscients qu'ils laissent sur les réseaux sociaux des informations personnelles pouvant être réutilisées à mauvais escient.

Un membre de la CNDP a ensuite rappelé que cette dernière était une institution récente, dont le mandat recouvre à certains égards une dimension pédagogique : son rôle consiste entre autres à diffuser la culture de la protection des données personnelle dans le pays. Il serait d'ailleurs préférable que la CNDP adopte une approche d'accompagnement, plutôt qu'une approche de sanction.

Enfin, le Maroc peut aisément disposer d'expertise internationale en matière de protection des données personnelles afin de se conformer à ses obligations légales et institutionnelles. Evidemment, il ne s'agit pas là de dupliquer les expériences internationales, mais plutôt d'en tirer des leçons et, si possible, d'adapter certains modèles au contexte marocain.

C. Recommandations des participants

Les discussions ont abouti aux recommandations suivantes :

SUR LE PLAN POLITIQUE

- Initier un dialogue inclusif entre toutes les parties concernées sur la protection des données personnelles dans le cadre du secteur de la sécurité
- Sensibiliser les citoyens sur la nécessité de protéger leurs données personnelles, ainsi que sur leurs droits en la matière
- Renforcer la connaissance des normes et bonnes pratiques internationales en matière de protection des données personnelles parmi les acteurs concernés
- Contribuer et soutenir le dialogue international relatif à la mise en place de mécanismes internationaux de protection des données personnelles
- Etablir une politique nationale de sécurité des systèmes informatiques
- Renforcer les mesures de cybersécurité et de cyberdéfense dans la stratégie nationale de sécurité
- Soutenir les entreprises innovantes en matière de cybersécurité

SUR LE PLAN JURIDIQUE

- Assurer la mise en conformité de la loi 09-08 avec la Convention 108 du Conseil de l'Europe
- Assurer de manière explicite l'indépendance de la Commission Nationale de contrôle de la protection des Données à caractère Personnel dans la loi 09-08
- Amender la loi 09-08 pour qu'elle encadre mieux le recours à des mesures intrusives (ex: vidéosurveillance)
- Adopter une loi régissant le droit d'accès à l'information et assurer sa conformité avec les normes et bonnes pratiques internationales
- Adopter une loi règlementant les interceptions administratives

Assurer la mise en conformité du Code de Procédure Pénale avec les engagements internationaux du Maroc en matière de protection des données personnelles (voir p. 21 pour les adhésions en cours)

Dans le cas des interceptions judiciaires et administratives, définir des mesures au degré d'intrusion grandissant selon la nécessité et le but à atteindre de sorte à respecter le principe de proportionnalité

Etablir un cadre juridique clair et précis relatif aux conditions de la levée du secret professionnel

Identifier et combler les vides juridiques relatifs au transfert international de données personnelles

SUR LE PLAN INSTITUTIONNEL

Augmenter le nombre de membres de la Commission Nationale de contrôle de la protection des Données à caractère Personnel et, si possible, éviter les doubles mandats

Renforcer la visibilité de la Commission Nationale de contrôle de la protection des Données à caractère Personnel par plus d'activités de communication externe

Renforcer les ressources financières et humaines de la Commission Nationale de contrôle de la protection des Données à caractère Personnel

Initier un dialogue inclusif entre toutes les parties concernées sur la protection des données personnelles dans le cadre du secteur de la sécurité

Faire évaluer les défis rencontrés par les institutions du secteur de la sécurité en matière de collecte et de traitement de données personnelles (efficacité et efficience du traitement, besoins financiers et humains)

Former les policiers à l'enregistrement et au traitement de plaintes relatives à la protection des données personnelles

Renforcer les moyens technologiques permettant de protéger les données personnelles au sein des institutions publiques (ex : cryptographie, meilleure gestion des accès et des utilisateurs)

Renforcer l'approche managériale de protection des données personnelles au sein des institutions publiques (ex : mise en place d'audit de sécurité périodiques)

Etablir des chartes et des codes déontologiques aussi bien pour les exploitants que pour les utilisateurs

SIÈGE DU DCAF, GENÈVE
Par poste:
Centre pour le contrôle démocratique des forces armées – Genève (DCAF)
P.O.Box 1360
CH-1211 Geneva 1
Suisse

Pour les visiteurs:
Centre pour le contrôle démocratique des forces armées – Genève (DCAF)
Chemin Eugène-Rigot 2E
CH-1202 Genève
Suisse
Tél : +41 (0) 22 741 77 00
Fax :+41 (0) 22 741 77 05
www.dcaf.ch

DCAF BEYROUTH
Gefinor Center - Block C – 6th Floor
Clemenceau Street
Beyrouth
Liban
Tél : + 961 (0) 1 738 401
Fax :+ 961 (0) 1 738 402

DCAF RAMALLAH
Al.Maaref Street 34
Ramallah / Al-Bireh
Cisjordanie
Palestine
Tél : +972 (2) 295 6297
Fax : +972 (2) 295 6295

DCAF TUNIS
14, rue Ibn Zohr
Cité Jardins – 1082
Tunis
Tunisie
Tél : +216 71 286 755
Fax : +216 71 286 865
tunis@dcaf.ch
www.dcaf-tunisie.org

DCAF TRUST FUND FOR NORTH AFRICA

Avec le soutien financier
du Fonds d'affection du DCAF
pour l'Afrique du Nord

DCAF
un centre pour la sécurité,
le développement et
l'état de droit