

## LA PROTECTION DES DONNÉES PERSONNELLES EN DROIT THAÏLANDAIS:

### ÉTAT DES LIEUX ET PERSPECTIVES\*

---

*Suppawat SINGSUWONG*

*Rapporteur au Conseil d'État de Thaïlande*

*Rapporteur adjoint du projet de loi sur la protection des données personnelles*

---

“*Vie privée : Aujourd’hui est demain*”. Tel est le mot d’ordre de la 31<sup>ème</sup> conférence internationale des autorités de protection des données et de la vie privée qui s’est tenue à Madrid en Espagne du 4 au 6 novembre 2009<sup>1</sup>. Le message est claire : il y a une nécessité pressante de réfléchir dès maintenant aux mécanismes appropriés de protection des données personnelles pour que le droit au respect de la vie privée soit effectivement garanti. C’est d’autant plus important qu’à notre époque les technologies de l’information et de communications sont en plein développement et les informations relatives aux individus sont collectées, utilisées et communiquées chaque jour, le plus souvent à l’insu des intéressés...

La protection de la vie privée est une préoccupation ancienne de la communauté internationale comme en témoigne la Déclaration universelle des droits de l’homme de 1948 qui reconnaît dans son article 12<sup>2</sup> le droit de l’individu à la protection de sa vie privée. Quant aux données personnelles qui sont l’un des aspects de la vie privée, leur protection est progressivement prévue dans une multitude de textes internationaux et régionaux dont le plus connu est probablement la Directive 95/46/CE de l’Union européenne relative à la protection des personnes physiques à l’égard du traitement des

---

\* TEXTE REMANIÉ ET ENRICHÉ DE LA COMMUNICATION PRÉSENTÉE À LA CONFÉRENCE FRANCOPHONE INTERNATIONALE ET RÉGIONALE SUR “*LES ENJEUX JURIDIQUES DU DÉVELOPPEMENT DES TECHNOLOGIES DE L’INFORMATION ET DE LA COMMUNICATION*”, HANOI VIETNAM, 18-19 NOVEMBRE 2009.

<sup>1</sup> Conférence à laquelle l’auteur de ces lignes a participé en tant que représentant de la Thaïlande.

<sup>2</sup> Article 12 *Nul ne sera l’objet d’immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d’atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.*

données à caractère personnel et à la libre circulation de ces données. Parallèlement, les droits nationaux de plus en plus nombreux tendent à instaurer le régime de protection des données personnelles.

Dans ce processus, l'Asie semble à la traîne par rapport aux autres régions du monde. Il n'y a que quatre pays ou territoires qui sont dotés de législation générale relative à la protection des données personnelles : le Japon<sup>3</sup>, Hong Kong<sup>4</sup>, Macao<sup>5</sup> et Taiwan<sup>6</sup> tandis que la Corée du Sud<sup>7</sup> et Singapour<sup>8</sup>, pays pourtant développés, en sont toujours dépourvus. De même pour la Chine où l'on remarque l'absence de législation dans ce domaine. Toutefois, il y a des pays qui font des efforts pour rattraper le retard. Aux Philippines, le *Data Privacy Bill* est en cours de discussion parlementaire. En Malaisie, le *Personal Data Protection Bill* a été finalement présenté au Parlement après de long processus d'élaboration. Enfin, le gouvernement thaïlandais a récemment approuvé le projet de loi sur la protection des données personnelles et va le transmettre au Parlement.

En Thaïlande, la Constitution actuelle, en vigueur depuis 2007, garantit dans son article 35 le droit de toute personne au respect de sa vie privée et interdit la production ou diffusion publiques d'une déclaration ou image qui pourraient y porter atteinte ainsi que le droit de toute personne à la protection contre l'exploitation illégale de ses données personnelles. C'est la première fois que le terme "données personnelles" fait apparition dans la loi suprême. Par ailleurs, l'article 56 de la même Constitution reconnaît le droit de toute personne d'accéder aux données détenues par les autorités publiques à l'exception des cas où la communication de ces données risquerait de porter atteinte aux intérêts ou données personnelles d'autrui. D'autres dispositions constitutionnelles contribuent également à la protection de la vie privée, comme l'article 36, qui en assurant la liberté de communication, interdit la censure,

---

<sup>3</sup> *Act on the Protection of Personal Information Held By Administrative Organs* 1998 pour le secteur public et *Act on the Protection of Personal Information* 2003 pour le secteur privé.

<sup>4</sup> *Personal Data (Privacy) Ordinance* 1995 pour les secteurs public et privé.

<sup>5</sup> *Computer Processed Data Protection Act* 1995 pour le secteur public et une partie du secteur privé

<sup>6</sup> *Personal Data Protection Act* 2006.

<sup>7</sup> *Act on the Protection of Personal Information Maintained by Public Agencies* 1999 assure la protection des données dans le secteur public alors que pour le secteur privé, *Act on Promotion of Information and Communication Network Utilization and Information Protection* 2001 n'est pas une loi de portée générale mais s'applique uniquement aux fournisseurs de services de télécommunications ainsi qu'aux certains secteurs d'activités comme les agences de voyage, compagnies aériennes et hôtels, etc.

<sup>8</sup> En l'absence de législation contraignante, la Cité-État se contente d'un *Model Data Protection Code for the Private Sector*, une sorte de code de bonne conduite qui sert d'instrument d'auto-régulation pour le secteur privé.

la rétention et la divulgation d'une communication entre personnes sauf en vertu des dispositions législatives visant spécifiquement la sécurité de l'État, la préservation de l'ordre public ou les bonnes mœurs.

Si le texte constitutionnel semble promouvoir la protection de la vie privée et des données personnelles, le niveau de protection dans l'ordre juridique thaïlandais laisse encore à désirer. En effet, la protection des données personnelles reste circonscrite au secteur public avec la loi de 1997 sur les renseignements publics qui fixe le régime juridique de protection des données personnelles détenues par les autorités publiques. Quant au secteur privé, la protection n'existe que pour certaines catégories de données personnelles comme celles relatives aux opérations de crédits ou celles des usagers des systèmes de télécommunications. D'où l'idée d'élaborer une loi générale sur la protection des données personnelles couvrant l'ensemble des données dans le secteur privé.<sup>9</sup> La Constitution a repris cette idée à son compte en énonçant à l'article 303 (1) que le gouvernement formé à la suite des premières élections générales sous cette constitution doit préparer un projet de loi sur les données personnelles dans le délai d'un an à compter de la date de la déclaration de politique générale au Parlement. C'est chose faite le 6 octobre dernier quand le Conseil des ministres a approuvé le projet de loi sur la protection des données personnelles dans sa version issue de l'examen du Conseil d'État.

Une fois approuvée par le Parlement et promulguée, cette loi constituera un complément logique aux lois de 2001 sur le commerce électronique et celle de 2007 sur la cybercriminalité<sup>10</sup>. Ce corpus de législations dans le domaine des TIC devrait assurer la "*confiance numérique*" des cybernautes, e-consommateurs et entreprises en ligne. Cela dit, il convient de préciser que cette loi ne concernera pas uniquement le traitement des données personnelles par les moyens informatiques. Elle aura une vocation générale et s'appliquera à toutes les données personnelles automatisés ou non qui sont en possession de toute personne – individus ou organismes de droit privé – à l'exclusion

---

<sup>9</sup> Le premier projet de loi en ce domaine a été élaboré dès 2001 par le Centre national de technologies électronique et informatique (NECTEC), un organisme rattaché au ministère de technologies de l'information et de communications.

<sup>10</sup> Certes, cette loi prévoit les sanctions pénales punissant toute personne qui, de manière illicite, a accédé aux données informatiques d'autrui ou a intercepté, endommagé, détruit, ou altéré ces données, lesquelles pouvant comporter les "données personnelles". Mais elle ne fixe pas directement les mesures de protection de ces données sans compter qu'elle a un objectif plus répressif que préventif et ne concerne que les données informatisées.

toutefois de celles détenues par des autorités publiques déjà sous le coup de la loi de 1997 sur les renseignements publics. Elle couvrira donc tous les secteurs d'activités : des établissements bancaires et financiers aux hôpitaux privés et compagnies d'assurance, en passant par les opérateurs touristiques et hôteliers, sans oublier les entreprises de vente directe. Ainsi cette loi répondra aux attentes des défenseurs de la vie privée qui rêvent depuis longtemps d'une protection juridique globale des données personnelles.

Dans le cadre de cette communication, nous ferons d'abord état de la protection des données personnelles telle qu'elle existe dans les législations actuelles avant de présenter les grandes lignes du projet de loi sur les données personnelles qui, une fois en vigueur, bouleversera le paysage juridique de la protection de la vie privée en Thaïlande.

## **I. Le défaut d'aujourd'hui : une protection insuffisante dans les législations actuelles**

À l'heure actuelle, la protection des données personnelles est insuffisante en ce qu'elle reste limitée au secteur public alors que les données dans le secteur privé ne bénéficient que d'une protection partielle.

### **A. Protection globale dans le secteur public**

À l'origine, les données personnelles dans le secteur public étaient protégées par les lois sectorielles comme la loi sur le registre d'état civil de 1991. Cette loi impose aux agents d'état civil d'assurer la protection des données relatives à l'état civil des personnes comme les nom, prénom, sexe, date de naissance et de décès, nationalité, religion, domicile, situation maritale, nom des parents, etc. Parmi les mesures de protection, on peut citer par exemple l'interdiction de communication publique de ces données sauf quelques cas d'exceptions comme le cas où il y a nécessité de préserver la sécurité de l'État. Il est également reconnu aux personnes intéressées le droit de demander la rectification, la suppression ou la mise à jour des données la concernant.

Par la suite, la loi de 1997 sur les renseignements publics a consacré la protection globale des données personnelles dans le secteur public. Cette loi a pour objet de promouvoir l'accès des citoyens aux "renseignements publics", c'est-à-dire ceux détenus par les autorités publiques (services des administrations centrale et provinciale, collectivités locales, entreprises publiques, etc.) Autrement dit, c'est une législation qui tend à assurer la transparence de l'administration à l'instar de la loi sur l'accès aux documents administratifs en France ou la *Freedom of Information Act* aux États-Unis. Cela dit, si elle n'a pas pour vocation principale la protection des données personnelles, elle n'en comporte pas moins de dispositions qui la concernent.

L'article 4 de la loi prend soin de donner la définition de "données personnelles" qui s'entend comme "*données relatives à l'identité d'une personne physique, par exemple celles relatives à l'éducation, situation financière, dossier médical, casier judiciaire, parcours professionnel, qui mentionnent le nom de cette personne ou qui comporte référence numérique, code ou autres indications permettant d'identifier ladite personne telles que les empreintes digitales, cassette ou disquette qui enregistre la voix de cette personne, sa photo, ainsi que les données relatives à l'identité de personne décédée.*"

La loi a fixé le régime de protection de ces données dans le troisième chapitre, de l'article 21 à l'article 25. Un régime qui peut se résumer en des principes suivants :

- Détermination des fins de la collecte : l'autorité publique est tenue d'informer la personne intéressée, avant ou lors de la collecte des données, des fins de leur utilisation ainsi que des conditions de leur utilisation normale. (art. 23 al. 2)

- Limitation de la conservation : l'autorité publique ne doit organiser le système de gestion des données personnelles qu'autant que celle-ci est nécessaire à la réalisation des objectifs de son fonctionnement et doit y mettre fin dès qu'il n'y en a plus de nécessité. (art. 23 al. 1 (1))

- Consentement lors de la communication : il est interdit à l'autorité publique détentrice des données personnelles de les communiquer à une autre autorité publique ou

toute autre personne sans accord écrit de la personne intéressée sous réserve des cas d'exception prévus par la loi.<sup>11</sup> (art. 24)

- Exactitude des données : l'autorité publique doit s'efforcer de recueillir les données personnelles directement de la personne intéressée, d'en vérifier régulièrement l'exactitude et rectifier le cas échéant les données erronées. (art. 23 al. 1 (2) et (4)) De son côté, la personne intéressée a également le droit de demander à l'autorité publique de rectifier ou supprimer les données erronées. (art. 25 al.3)

- Mesures de sécurité : le système de gestion des données personnelles doit être doté des mesures de sécurité destinées à prévenir tout risque d'utilisation illicite ou d'éventuel préjudice. (art. 23 al. 1 (5))

- Transparence dans la gestion des données : l'autorité publique doit veiller à ce que les informations relatives à la gestion des données personnelles soient publiées au Journal Officiel et qu'elles soient régulièrement vérifiées et rectifiées.<sup>12</sup> (art. 23 al. 1 (3))

- Accès aux données personnelles : toute personne dispose du droit d'accès aux données personnelles la concernant. Sur demande écrite de l'intéressé, l'autorité publique est tenue de l'autoriser à consulter les données ou de lui en délivrer la copie. (art. 25 al.1)

- Droit de recours : la personne intéressée a droit de former un recours contre le refus de l'autorité publique d'autoriser la consultation de ses données personnelles ou le refus de rectifier ou de supprimer les données erronées, respectivement devant la Commission de renseignements publics et la Commission de communication des renseignements. (art. 13 et art. 25 al. (4))

Au total, la loi sur les renseignements publics offre un cadre juridique plutôt complet pour la protection des données personnelles dans le secteur public même s'il existe certains points sur lesquels elle reste silencieuse comme le transfert des données à l'étranger. Une telle protection fait encore défaut dans le secteur privé qui reste régi par

---

<sup>11</sup> Parmi ces cas d'exception, on peut citer par exemple le cas où la communication est nécessaire à la prévention ou l'éradication des dangers menaçant la vie ou la santé des personnes ou la communication à des fins de recherche sans aucune mention de nom ou autre indication qui permet d'identifier la personne intéressée.

<sup>12</sup> Ces informations sont par exemple les conditions d'utilisation normale des données, la procédure de consultation des données, celle relative à la demande de rectification des données, etc.

les législations sectorielles, lesquelles ne couvrent qu'une infime partie des données personnelles détenues par les entreprises privées.

### **B. Protection partielle dans le secteur privé**

Il existe des lois qui permettent la protection des données personnelles dans certains secteurs d'activités telles que la loi de 2002 sur la gestion des données relatives aux opérations de crédits et la loi de 2001 sur les activités de télécommunication.

La première loi impose aux sociétés de gestion des données relatives aux opérations de crédits de mettre en place les mesures de traitement ayant trait aux collecte, enregistrement, conservation, utilisation, communication et suppression des données. L'utilisation des données par les banques et organismes financiers est strictement limitée à l'examen pour l'octroi d'un prêt et les données ne peuvent être communiquées aux personnes non autorisées. Le responsable des fichiers de données ont l'obligation de prendre les précautions utiles pour assurer la sécurité des données. Par ailleurs, le droit d'accès au fichier et à la rectification des données est également reconnu aux personnes concernées.

La seconde loi impose à la Commission Nationale d'Activités de Télécommunication (CNAT) de fixer les mesures de protection des données des usagers des moyens de télécommunication, de leur droit à la vie privée et liberté de communication par les moyens de télécommunication. En 2006, la CNAT a publié l'arrêté fixant les mesures susmentionnées dont les grandes lignes rappellent, à bien des égards, les principes de protection des données personnelles de la loi de 1997 sur les renseignements publics. Le traitement des données personnelles est soumis à l'accord de l'utilisateur et doit se faire uniquement pour le besoin des activités de télécommunication. L'opérateur est tenu de recueillir les données directement de l'utilisateur et la collecte est limitée au besoin des activités de télécommunication et aux buts conformes aux dispositions légales. La collecte est interdite pour certaines "données sensibles", par exemple l'incapacité physique ou caractéristiques génétiques de l'individu. L'opérateur ne peut conserver les données de l'utilisateur au delà d'une durée de deux ans à compter de la date où il a cessé de lui fournir le service de télécommunication. L'utilisateur dispose du droit d'accès

aux données le concernant, d'en demander la rectification, de demander la cessation de l'utilisation ou de la communication des données ainsi que de retirer son accord pour le traitement des données à tout moment.

Dans d'autres secteurs d'activités, il existe des lois qui prévoient les règlements sur la déontologie et l'obligation de confidentialité des professions réglementées à l'égard des données personnelles de leurs clients telles que la loi de 1960 sur la profession d'experts-comptables, celle de 1985 sur la profession d'avocats ainsi que différentes lois sur les professionnels de santé (médecins, chirurgiens-dentistes, pharmaciens, infirmières et sages-femmes). Cependant, ces règlements ont le contenu trop général et la force juridique incertaine, ce qui ne permet pas une protection effective des données personnelles des individus.

Face à cette carence, on serait tenté de recourir aux dispositions des codes civil et pénal sur la responsabilité quasi-délictuelle ou la diffamation, mais leur utilité est limitée car elles sont de nature plus réparatrice ou répressive que préventive. En outre, sous le régime de droit commun, la charge de la preuve incombe le plus souvent à la personne qui a subi les préjudices, ce qui est loin de faciliter l'action en justice.

Cette protection des données personnelles par les lois sectorielles n'est pas sans rappeler la situation des États-Unis qui n'ont pas toujours de loi générale en ce domaine mais prennent l'option d'une protection par secteurs d'activités ou par catégories de personnes à protéger.<sup>13</sup> Une telle position n'est pas partagée par la majorité des pays européens qui ont choisi la voie d'une protection globale par l'adoption de loi générale. C'est dans cette dernière direction que la Thaïlande se résout à s'engager en élaborant le projet de loi sur la protection des données personnelles, une législation qui vise à protéger les données personnelles dans l'ensemble du secteur privé.

---

<sup>13</sup> Par exemple Cable TV Privacy Act 1984 pour les données personnelles des souscripteurs de télévision par câble, Video Privacy Protection Act (VPPA) 1988 pour les données des clients de magasin de location de cassettes vidéo, Children's Online Privacy Protection Act 1998 (COPPA) pour les données personnelles des mineurs de moins de 13 ans. , etc.

## **II. Le défi de demain : une protection renforcée par la loi sur les données personnelles**

L'idée d'une loi générale sur la protection des données personnelles remonte à l'année 2001. Mais les désaccords entre les services administratifs et les changements politiques ont retardé son élaboration. Le projet de loi a été préparé par l'Office de la Commission des Renseignements Publics à la suite d'un rapport d'étude préparé par une équipe de professeurs de la faculté de droit de l'université Thammasat. En 2006, le projet de loi a été présenté au Conseil des ministres et soumis à l'examen du Conseil d'État.

De point de vue de droit comparé, le Conseil d'État a examiné le projet de loi en considérant plusieurs législations étrangères, notamment la loi fédérale du Canada sur la protection des renseignements personnels et les documents électroniques de 2000 (PIPEDA), la loi suédoise sur les données personnelles de 1998 (Personal Data Act) et la loi fédérale allemande sur la protection des données de 1990 (Bundesdatenschutzgesetz, BDSG)

À l'issue de l'examen du Conseil d'État, le texte a été substantiellement modifié, et ce dans le sens d'une plus grande protection des données personnelles. Nous n'avons pas l'ambition d'exposer ce projet dans tous les détails mais simplement d'en présenter les traits saillants. Ce texte est caractérisé par son champs d'application vaste et son régime de protection stricte, des caractéristiques qui méritent quelques observations et commentaires.

### **A. Un champs d'application vaste**

Le projet de loi reprend la définition de "données personnelles" de la loi sur les renseignements officiels de 1997 et il s'applique à *toutes les données personnelles en possession de tout individu et personne morale de droit privé*. Les données personnelles détenues par les autorités publiques en sont exclues car déjà régies par la loi sur les renseignements publics de 1997. Particularité notable : les entreprises publiques, déjà sous le coup de la loi de 1997, sont également incluses dans le champs d'application de la loi sur les données personnelles. La raison est que dans certains secteurs d'activités, les entreprises publiques, notamment celles sous forme de société

anonyme, sont en concurrence avec des entreprises privées.<sup>14</sup> Il faudrait donc les placer toutes les deux sous le même régime juridique contraignant pour ne pas fausser la concurrence. Ainsi, les entreprises publiques seront soumises à deux législations à la fois : la loi sur les renseignements officiels de 1997 en tant qu'« autorité publique » et la loi sur la protection des données personnelles en tant que société opérant dans le secteur privé.

Par ailleurs, la loi ne s'applique pas aux données personnelles que les personnes physiques ou morales recueillent pour des fins personnels sans laisser d'autres personnes utiliser ces données ou les communiquer à autrui. Sont également exclues du champ d'application de la loi l'utilisation et la communication des données personnelles recueillies à *des fins journalistiques, artistiques ou littéraires*. On peut regretter cette dernière exception qui n'est assortie d'aucun tempérament. Certes, les libertés d'expression et de la presse sont les libertés fondamentales reconnues par l'article 45 de la Constitution. Mais le même article permet qu'une loi puisse apporter des restrictions à l'exercice de ces libertés si elle a pour but de protéger la vie privée d'autres personnes...

En tant que loi générale, la loi sur la protection des données personnelles s'appliquera à toute opération relative aux données personnelles qui n'est régie par aucune loi particulière. Cela dit, même dans le cas où il existe des dispositions de loi spécifique qui fixe les règles concernant une opération donnée, le Premier ministre, avec l'approbation du Conseil des ministres, peut édicter un arrêté ordonnant l'application des dispositions de la loi sur la protection des données personnelles, *en complément ou en remplacement* des dispositions de la loi spécifique s'il existe un motif valable.<sup>15</sup> Ce mécanisme de substitution met parfaitement en lumière la vocation *générale* de la loi sur la protection des données personnelles.

En dernier lieu, il convient de noter que le Conseil d'État a apporté une importante modification au texte originel en élargissant le champ d'application de la loi : celle-ci s'appliquera à toute opération relative aux données personnelles, *y compris*

---

<sup>14</sup> On pense particulièrement aux Thai Airways International dans le secteur de transport aérien, Krungthai Bank dans le secteur bancaire, CAT Telecom dans le secteur de télécommunications, TOT dans le secteur de téléphonie et PTT dans le secteur pétrolier.

<sup>15</sup> On s'inspire du mécanisme existant dans certaines législations comme la loi sur les substances dangereuses de 1992.

*celle dans le cadre d'une activité sans but lucratif ou commercial* alors qu'à l'origine, seules les activités lucratives et commerciales y étaient soumises. Cet extension du champs d'application de la loi est conforme à l'esprit de l'article 35 de la Constitution qui a pour objectif la protection contre toute exploitation illégale des données personnelles, cela sans considération de la nature des activités concernées.

## **B. Un régime de protection stricte**

### **• Des principes classiques mais plus sévères**

Si on retrouve les principes existants dans la loi sur les renseignements publics de 1997, le régime de protection de la loi sur les données personnelles est, dans son ensemble, plus sévère que celui de sa devancière. Sans prétendre à l'exhaustivité, on peut mentionner quelques points de repères :

- Consentement de l'intéressé : on exige le consentement de la personne intéressée avant ou lors de toute opération relative à ses données personnelles, qu'il s'agisse de collecte, utilisation ou communication des données. Pour que le consentement soit valable, l'intéressé doit être préalablement informé des fins de l'opération envisagée. Par ailleurs, l'intéressé dispose du droit de se rétracter avec possibilité de retirer son consentement à tout moment sous réserve de disposition légale ou clause contractuelle restreignant l'exercice de ce droit.

La loi prévoit quelques exceptions au principe du consentement. Celles-ci sont de deux ordres. D'une part, les exceptions communes à toutes les opérations. Par exemple le cas où l'opération est dans l'intérêt de l'intéressé et il est impossible de demander son consentement sur le champs ou il s'agit de sauvegarder la vie, la santé ou la sécurité de l'intéressé. D'autre part, les exceptions propres à chaque opération. Par exemple, pour la collecte des données, le consentement de l'intéressé n'est pas nécessaire s'il s'agit des données recueillies lors de spectacle, manifestation sportive ou autres activités de même nature à condition que la personne intéressée y apparaisse ou participe de sa propre volonté et il s'agit d'activités ouvertes au public. Quant à la communication des données,

le consentement n'est pas exigé lorsqu'elle est faite à l'avocat qui représente le responsable du traitement des données ou qu'elle est faite en vue de recouvrement d'une créance que celui-ci a contre l'intéressé ou encore quand elle est faite à un organisme chargé de la conservation de documents historiques.

- Limitation de la conservation : le responsable du traitement des données ne peut conserver les données personnelles au-delà de la durée initialement notifiée à l'intéressé ou la durée exigée par les fins de la collecte. Au terme desdites durées, il est tenu de supprimer les données ou les rend insusceptibles d'identifier la personne intéressée. Cela dit, il peut continuer à conserver les données pour des fins de statistiques ou de recherche s'il obtient l'accord écrit de l'intéressé.

- Mesures de sécurité : le responsable du traitement des données doit mettre en œuvre les mesures de sécurité appropriées pour protéger les données personnelles contre l'utilisation ou la communication illicites qui seraient préjudiciables à l'intéressé, la perte, l'altération, l'accès non autorisé et la destruction des données. Ces mesures devant concerner au moins l'accès et l'utilisation du système informatique, le plan d'urgence en cas de panne informatique ainsi que la vérification et l'évaluation des risques concernant le système informatique.

- Droits de la personne intéressée : celle-ci dispose du droit d'accès aux données personnelles la concernant ainsi que celui d'en demander la rectification, la mise à jour et la suppression.

#### ● **Des innovations bienvenues**

Le projet de loi sur la protection des données personnelles comporte quelques nouveautés par rapport à la loi sur les renseignements publics de 1997. Parmi les aspects novateurs, citons par exemple :

- Régime des "données sensibles" : la loi fixe de manière expresse les règles gouvernant la collecte, l'utilisation et la communication des "données sensibles". Ces dernières sont notamment les données relatives à la vie sexuelle, casier judiciaire, origines ethniques ou raciales, opinions politiques, croyances religieuses de l'individu

telles que définies par l'arrêté ministériel. Elles bénéficient d'une protection plus grande que les données ordinaires en ce sens que leur collecte, utilisation ou communication nécessite l'accord écrit de l'intéressé et que les exceptions au principe du consentement sont limitées au strict minimum.

- Régime de transfert de données à l'étranger : le texte prévoit les règles concernant le transfert de données personnelles à l'étranger. On y trouve l'influence de la Directive 95/46/CE de l'Union européenne et des législations des pays européens. Le transfert des données est soumis à l'accord écrit de la personne intéressée. Il n'est permis d'y déroger que dans certains cas d'exceptions, par exemple, lorsque le transfert est nécessaire à l'exécution d'un contrat entre la personne intéressée et le responsable du traitement ou à l'exécution du contrat entre le responsable du traitement et un tiers dans l'intérêt de la personne intéressée ou lorsque le transfert est nécessaire pour prévenir et réprimer le blanchiment d'argent et les actes de terrorisme. En l'absence de l'accord écrit de la personne intéressée, il est également interdit d'effectuer un transfert de données vers *un pays qui n'est pas doté de législation protectrice des données personnelles ou celui dont la législation offre un niveau de protection inférieur à la protection nationale*. Notons que cette condition est plus stricte que celle posée par la Directive 95/46/CE qui n'exige qu' "*un niveau de protection adéquat*".

- Régime spécial pour certaines catégories de responsables du traitement :

un régime de protection plus rigoureux est prévu pour les "*responsables du traitement des données personnelles exerçant des activités commerciales*". Ces activités seront déterminées ultérieurement par l'arrêté ministériel mais on pense déjà aux secteurs d'activités où la collecte des données personnelles sont monnaie courante avec le risque d'atteinte à la vie privée. Toutefois, il est fort probable que l'on ne retiendra que "*les plus grandes entreprises*", en se basant, par exemple, sur le montant des chiffres d'affaires, le nombre d'employés ou le nombre des données personnelles conservées. Hormis les obligations générales auxquelles tous les responsables du traitement sont soumis, les *responsables du traitement exerçant des activités commerciales* seront tenus par les contraintes supplémentaires comme celles d'établir les politiques ou codes de conduite pour le traitement des données au sein de l'organisme (*privacy policy*), de mettre en place

le système de sécurité ou encore d'organiser les formations de leurs employés dans le domaine de protection des données. Notons également qu'en cas de sous-traitance, il leur incombe de prévoir dans le contrat les mesures qui garantissent le niveau de protection au moins égales à celles prévues par la loi et les règlements d'application.

### ● **Des organes de contrôle aux pouvoirs étendus**

La loi prévoit la création de la Commission de Protection des Données Personnelles, laquelle peut installer une ou plusieurs "commission(s) de surveillance des données personnelles"

#### - La Commission de Protection des Données Personnelles (CPDP)

C'est une instance collégiale composée de 13 membres comprenant les hauts fonctionnaires, représentants du secteur privé et experts dans le domaine du droit et de technologie. Elle a le pouvoir de fixer les politiques et mesures de protection des données, donner des avis et recommandations, édicter les arrêtés d'application de la loi ainsi que le code de conduite fixant les bonnes pratiques à destination des responsables du traitement des données. Question logistique, l'Office de la Commission des Renseignements Publics, déjà responsable de la protection des données dans le secteur public, servira de secrétariat pour la future Commission de Protection des Données Personnelles. Situation un peu curieuse si l'on songe qu'en France, la CADA et la CNIL devaient partager les mêmes services administratifs, qui de plus sont sous l'égide de l'Office du secrétariat général de l'Office du Premier ministre et donc perméable à toute ingérence politique... Mais il s'agit sans doute d'une solution provisoire avant l'avènement d'une *autorité indépendante* dans le domaine de la protection des données personnelles.

#### - Les commissions de surveillance des données personnelles

Si la CPDP est une instance de politique et d'orientation, les commissions de surveillance, quant à elles, assureront le travail au quotidien en matière de protection des données personnelles. Elles sont chargées d'examiner les réclamations relatives aux violations de la loi, de mener les investigations sur les cas allégués et tenter de

concilier les protagonistes. Si les faits sur les violations de la loi sont établis et les tentatives de conciliation ont échoué, la commission peut enjoindre au responsable du traitement des données de se conformer aux prescriptions légales. Cette injonction étant un acte administratif, si le contrevenant n'obtempère pas dans le délai imparti, la commission peut infliger des "amendes administratives" (astreintes journalières) au récalcitrant et en cas de non paiement, de procéder au recouvrement forcé des amendes, ceci conformément aux dispositions de la loi sur la procédure administrative non contentieuse de 1996. Les décisions de la commission – qu'il s'agisse de fin de non recevoir opposé à l'auteur de la réclamation ou l'injonction au responsable du traitement – sont susceptibles d'appel devant la Commission de Protection des Données Personnelles.

### • Des mesures de protection variées

Pour protéger de manière effective les données personnelles, la loi prévoit toute une gamme de mesures allant de la récompense à la punition en passant par la réparation.

Au titre de mesures incitatives et de soutien, le responsable du traitement des données peuvent solliciter les conseils en matière de protection des données personnelles ainsi que les aides aux formations de leurs employés. Par ailleurs, les responsables du traitement agréés peuvent demander l'octroi de "*marque de garantie de la protection des données personnelles*", un label de qualité grâce auquel on peut gagner la confiance des clients et usagers soucieux de la protection de leur vie privée.

À propos de l'arsenal répressif, on dénote une nette préférence pour les sanctions administratives en raison de la célérité du procédé et de la volonté de ne pas pénaliser les délits mineurs. En effet, la grande majorité des infractions sont passibles d'amendes administratives dont le montant dans certains cas peut atteindre 100,000 bahts C'est le directeur de l'Office de la Commission des Renseignements Publics qui dispose du pouvoir d'infliger les amendes administratives dont le montant devrait se calculer en fonction de la gravité de l'acte et l'importance du dommage causé. Les sanctions pénales - amendes pénales et emprisonnement – sont réservées uniquement aux infractions les plus graves, conformément à la politique de dépenalisation.

Enfin, est également prévue la responsabilité civile des responsables du traitement des données dont le régime est plus stricte que celui de droit commun. À ce propos, on peut cependant déplorer qu'il n'y ait pas l'introduction de "*punitive damages*" comme mesure à la fois restitutive et répressive pour prévenir l'atteinte à la vie privée (sur ce point, on pense - pour une fois - au système américain) car le montant de ces dommages-intérêts punitifs serait beaucoup plus dissuasif par rapport à ceux qui sont traditionnellement alloués par les tribunaux.

Le projet de loi sur la protection des données personnelles est le fruit d'un travail de longue haleine qui a associé tout au long de son processus d'élaboration tous les milieux intéressés : le monde universitaire, les administrations, les experts en TIC et surtout les représentants de la société civile et des secteurs économiques. Notons que ces derniers

avaient l'opportunité, lors de la consultation publique, de présenter leur observations et réserves dont certaines ont été prises en compte par le Conseil d'État et conduisent à la modification des dispositions concernées. Au final, il en résulte un texte plutôt équilibré qui vise à une protection maximale de la vie privée des individus tout en aménageant les marges de manœuvre aux entreprises pour ne pas trop entraver la marche des affaires. En tant que positiviste, nous pensons qu'il a réussi à concilier « *l'ordre et le progrès* ». Souhaitons qu'il trouvera grâce aux yeux du législateur et des citoyens.

En conclusion, on peut dire que la protection de la vie privée peut être assurée de différentes manières. La plupart du temps, elle peut prendre la forme de l'auto-régulation avec l'édiction par les entreprises de codes de bonne conduite ou "*privacy policy*". Une pratique qui peut être appuyée par le développement des logiciels et programmes d'application informatiques soucieux de respecter la vie privée et les données personnelles, c'est le fameux concept de "*privacy by design*"<sup>16</sup>. Mais le plus souvent les bonnes volontés et l'ingéniosité technique ne suffisent plus et il faudrait l'intervention de l'État pour fixer les règles du jeu et créer une autorité publique pour veiller à leur respect.

À l'heure actuelle, il est encore trop tôt pour faire un pronostic sur l'avenir du projet de loi sur les données personnelles. Certes, cette loi sera certainement promulguée car le législateur a l'obligation constitutionnelle de l'édicter. Mais son contenu risque d'être altéré en cours de discussions parlementaires et ce dans le sens d'une moindre protection pour les données personnelles. C'est maintenant aux représentants du peuple de donner le verdict. Espérons qu'il ira dans le bon sens car la vie privée des citoyens en dépend.

Plus que jamais il faut garder à l'esprit : "*Aujourd'hui est demain*".

---

<sup>16</sup> Concept inventé dans les années 1990 par Ann Cavoukian, commissaire à la vie privée d'Ontario au Canada. Pour le dernier développement cf. "*Privacy by design ... Take the challenge*", 2009.