COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, le 16 octobre 2017 T-PD(2017)17

COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT AUTOMATISÉ DES DONNÉES À CARACTÈRE PERSONNEL

AVIS SUR LA DEMANDE D'ADHÉSION DES ÉTATS-UNIS DU MEXIQUE

Direction générale des droits de l'homme et de l'État de droit

Introduction

Le 28 août 2017, le Secrétaire général du Conseil de l'Europe a reçu une lettre datée du 25 août 2017 lui faisant part du souhait des États-Unis du Mexique d'adhérer à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ci-après "Convention 108" ou "la Convention") et au Protocole additionnel à la Convention, concernant les autorités de contrôle et les flux transfrontières de données (ci-après "Protocole additionnel").

Le Comité consultatif de la Convention 108 rappelle qu'il avait en 2008 porté à l'attention du Comité des Ministres sa recommandation visant à inviter à adhérer à la Convention 108 les États non membres ayant en matière de protection des données une législation conforme à cette Convention. Les Délégués des Ministres avaient pris acte de cette recommandation et décidé d'examiner toute demande d'adhésion à la lumière de celle-ci (1031ème réunion, 2 juillet 2008).

Avis

Conformément à l'article 4 de la Convention 108, chaque Partie prend, dans son droit interne, les mesures nécessaires pour donner effet aux principes de base pour la protection des données énoncés dans la Convention (chapitre II). En vertu de l'article 3.1 du Protocole additionnel, les Parties considèrent les dispositions des articles 1 et 2 du Protocole comme des articles additionnels à la Convention, et toutes les dispositions de la Convention s'appliquent en conséquence.

Après avoir pris note de la Constitution des États-Unis du Mexique (articles 1, 16§2, 6A-II, III et VIII, 73, 116 et 133) qui garantissent, respectivement, la jouissance des droits de l'homme, les droits au respect de la vie privée et à la protection des données à caractère personnel, les droits des personnes concernées (accès, modification, effacement, objection), l'institution d'un organisme autonome et indépendant chargé de faire respecter le droit à la protection des données à caractère personnel ("l'Institut national de la transparence, de l'accès à l'information et de la protection des données à caractère personnel", ci-après "INAI"), sa composition, la compétence législative en la matière du Congrès de l'Union des États-Unis du Mexique et la place occupée par les traités internationaux dans l'ordre juridique interne.

Après avoir examiné[1] la loi fédérale de 2010 sur la protection des données à caractère personnel détenues par les parties privées (ci-après "la loi fédérale"), le règlement d'application de 2010 de la loi fédérale sur la protection des données à caractère personnel détenues par les parties privées (ci-après "le règlement") et la loi générale de 2017 sur la protection des données à caractère personnel détenues par les parties soumises à obligation (ci-après "la loi générale"), le Comité constate ce qui suit.

1. Objet et but (article 1er de la Convention 108)

L'article 1er de la loi fédérale énonce son objet : *"protéger les données à caractère personnel détenues par les parties privées, dans le but d'en réglementer le traitement légitime, contrôlé et*

[1] Textes législatifs soumis avec la demande :

- https://mycloud.coe.int/index.php/s/MRj0JVXMXeyxTGy
- https://mycloud.coe.int/index.php/s/9360xnCcX5jAMrw

Sur la base d'une traduction en anglais des lois et règlements, dont les versions originales sont disponibles aux adresses suivantes :
La loi fédérale : http://inicio.ifai.org.mx/LFPDPPP/LFPDPPP.pdf
Le règlement d'application : http://inicio.ifai.org.mx/PROTECCIONDEDATOSPERSONALES/RLFPDPP.pdf
La loi générale : http://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017

éclairé, afin de garantir la vie privée et le droit à l'autodétermination en matière d'information des personnes physiques".

L'article 1er de la loi générale énonce son objet en indiquant que cette loi représente "*les dispositions destinées à faire appliquer les articles 6A et 16, deuxième paragraphe de la Constitution politique des États-Unis du Mexique, concernant la protection des données à caractère personnel détenues par les parties soumises à obligation*" et qu'elle "*vise à établir les bases, les principes et les procédures nécessaires pour défendre le droit de toute personne à la protection des données à caractère personnel la concernant détenues par les parties soumises à obligation*".

Ces indications sont conformes au but énoncé dans les dispositions de l'article 1er de la Convention 108.

2. Définitions

La loi fédérale définit les "données à caractère personnel", le "traitement des données" et la "personne chargée de contrôler les données" (articles 2 a, 2 b et 2 d de la Convention 108) dans ses articles 3(V), 3(XVIII) et 3(XIV), respectivement. Cette loi définit également les notions de "données sensibles" dans son article 3(VI), de "personne chargée du traitement des données" dans son article 3(IX), de "propriétaire des données" dans son article 3(XVII) et de "transfert'' dans son article 3(XIX). Le règlement d'application ajoute un certain nombre de définitions à celles que propose la loi fédérale, en définissant notamment les notions de "personne physique identifiable" et de "transmission" (article 2 du règlement).

La loi générale énonce des définitions analogues et incorpore en outre les définitions des notions d'évaluation de l'incidence sur la protection des données à caractère personnel" dans son article 3(IV), de consentement dans son article 3(VIII) et de système de classement dans son article 3(XII).

A. Données à caractère personnel (article 2 a de la Convention)

La loi fédérale définit les "données à caractère personnel" comme "*toute information concernant une personne physique identifiée ou identifiable*" dans son article 3(V).

La loi générale énonce dans son article 3(XXI) une définition analogue en ajoutant qu'"*une personne physique est réputée identifiable lorsque son identité peut être directement ou indirectement inférée de toute information*".

Les deux lois définissent la personne concernée (appelée 'propriétaire des données' dans la loi fédérale) comme "*la personne physique concernée par les données à caractère personnel*".

Cette définition correspond à celle qui figure dans l'article 2 a de la Convention 108.

B. Traitement automatisé (article 2 c of the Convention)

L'article 3(XVIII) de la loi fédérale définit "le traitement des données à caractère personnel" comme "*l'extraction, l'utilisation, la divulgation ou l'enregistrement de données à caractère personnel à l'aide de tous procédés. L'utilisation s'entend de toute opération d'accès, de gestion, d'exploitation, de transfert ou de destruction de données à caractère personnel*".

La loi générale présente une définition plus complète du traitement des données dans son article 3(XXIV) : "*Toute opération ou tout ensemble d'opérations effectuées à l'aide de procédés manuels ou automatisés appliqués à des données à caractère personnel, et concernant l'extraction, l'usage, la consignation, l'organisation, la conservation, la préparation, l'utilisation, la communication, la diffusion, l'enregistrement, le stockage, l'accès, la gestion, l'exploitation, la mise à disposition, le transfert ou la destruction de données à caractère personnel*".

L'article 2 c de la Convention 108 incorpore des opérations supplémentaires dans la liste non limitative, qui mentionne également l'"application d'opérations logiques et/ou arithmétiques" aux données traitées et la "modification" et l'"effacement" de ces données. Le Comité considère que la définition de la loi fédérale peut être interprétée comme une définition plus étroite (la loi générale mentionne 'tout opération ou tout ensemble d'opérations' relatives à une liste d'actions particulieres, ce qui apparait plus étroit également) qui gagnerait à être complétée, s'agissant en particulier des opérations susmentionnées que la définition n'énumère pas.

C. Maître du fichier (article 2 d de la Convention)

Dans son article 3(XIV), la loi fédérale définit la personne chargée de contrôler les données comme "*la personne physique ou la personne morale privée qui décide du traitement des données à caractère personnel*". La loi générale donne une définition analogue dans son article 3(IX), mis à part le fait qu'elle s'applique aux parties soumises à obligation.

Il serait utile d'élargir cette définition de manière à lui faire détailler les opérations effectuées qui aident à identifier la personne chargée de contrôler les données conformément à l'article 2 d de la Convention 108, c'est-à-dire la prise de décisions sur la finalité, les catégories de données à caractère personnel concernées et les opérations à leur appliquer.

D. Catégories particulières de données (article 6 de la Convention)

Les "données sensibles" sont définies dans l'article 3(VI) de la loi fédérale comme "*(l)es données à caractère personnel qui concernent les aspects les plus personnels de la vie privée du propriétaire de données ou dont la mauvaise utilisation pourrait aboutir à une discrimination à son égard ou lui faire courir un risque grave. Sont, en particulier, considérées comme sensibles les données pouvant révéler des aspects tels que l'origine raciale ou ethnique, l'état de santé actuel ou futur, les données génétiques personnelles, les convictions religieuses, philosophiques et morales, l'appartenance à un syndicat, les opinions politiques et la préférence sexuelle*." La loi générale donne une définition analogue dans son article 3(XXVIII).

Cette définition est conforme à l'article 6 de la Convention (si les données à caractère personnel concernant des condamnations pénales ne sont pas expressément mentionnées dans cet article, la liste qui y figure n'est pas exhaustive, comme le dénote l'expression 'en particulier'). Au reste, ces données sont couvertes par un chapitre spécifique de la loi générale (articles 80 à 82) qui prescrit un système de classement spécifique assorti de garanties renforcées en matière de sécurité.

Le Comité note enfin que la définition de « transfert » dans la loi fédérale (article 3, XIX) et dans la loi générale (Titre V) ne concerne pas seulement les flux transfrontières, comme dans le cas de l'article 12 de la Convention et l'article 2 de son Protocol Additionnel, mais aussi les opérations nationales.

3. Champ d'application du régime de protection des données (article 3 de la Convention)

L'article 1er de la loi fédérale protège les "données à caractère personnel détenues par les parties privées", tandis que l'article 1er de la loi générale garantit la "protection des données à caractère personnel détenues par les parties soumises à obligation", c'est-à-dire "*toute autorité ou entité, tout service ou organisme des pouvoirs exécutif, législatif et judiciaire, toute entité autonome, tout parti politique, toute fiducie et tout fonds public*" ainsi que les "*syndicats et tout autre particulier ou toute autre personne morale recevant et utilisant des fonds publics ou remplissant des fonctions d'autorité aux échelons fédéral, des États fédérés ou local*" (voir l'article 1er, paragraphes 5 et 6 de

la loi générale). Les buts de la loi générale sont également décrits dans son article 2. Il s'ensuit que le régime de protection des données s'applique à la fois au secteur privé (la loi fédérale) et au secteur public (la loi générale). Ce champ d'application correspond à celui qui fait l'objet de l'article 3 de la Convention 108.

"*Les personnes procédant à la collecte et à l'enregistrement de données à caractère personnel pour un usage exclusivement personnel et non à des fins de diffusion ou pour un usage commercial*" ne relèvent pas du champ d'application de la loi fédérale (article 2(II) de la loi fédérale), ce qui est conforme à l'article 3 du projet de convention 108 modernisée[2].

La loi fédérale ne précise pas qu'elle s'applique "au traitement automatisé ou non non automatisé des données à caractère personnel", et ce double critère n'est pas non plus mentionné dans la définition du traitement (contrairement à ce qu'il en est pour la loi générale, qui mentionne expressément les "*moyens manuels ou automatisés*" dans la définition du traitement).

En outre, l'article 2 de la loi fédérale dispose que les "firmes effectuant des enquêtes sur la solvabilité relevant de la loi réglementant les firmes effectuant des enquêtes sur la solvabilité et des autres lois applicables" ne relèvent pas de la loi fédérale, mais d'une *lex specialis*[3], qui ne contient pas de dispositions expresses relatives à la protection des données, ce qui implique que les droits de la personne concernée conférés par la loi fédérale ne sont pas reconnus dans le contexte des enquêtes sur la solvabilité, ce qui mériterait d'être revu.

Le Comité est d'avis que le libellé de la loi fédérale pourrait être révisé pour montrer clairement qu'il importe, en ce qui concerne le champ d'application, de couvrir à la fois le traitement automatisé et le traitement non automatisé.

La loi générale s'applique à "*tout traitement de données à caractère personnel sur support physique ou électronique, quel que soit le mode de création de ces données, le type de support, le traitement, l'enregistrement et l'organisation*" (article 4). Cette disposition apparaît conforme à l'article 3 de la Convention 108.

La loi fédérale comme la loi générale font référence aux sources accessibles au public. Le Comité note qu'il serait bon de préciser que la législation sur la protection des données s'applique aux données à caractère personnel figurant dans ces sources.

En ce qui concerne le journalisme, le Comité constate que la loi fédérale ne prévoit aucune dérogation au champ d'application des exigences en matière de protection des données.

4. Qualité des données (article 5 de la Convention)

L'article 6 de la loi fédérale prévoit que les "*(l)es personnes chargées de contrôler les données doivent respecter les principes de légalité, consentement, notification, qualité, finalité, fidélité, proportionnalité et responsabilité établis par la loi*." De plus, l'article 7 garantit que les données à caractère personnel sont obtenues et traitées loyalement et licitement. L'article 11 garantit que les données sont pertinentes, exactes et à jour et sont conservées pendant une durée n'excédant pas celle nécessaire pour atteindre l'objectif recherché (le Comité note que l'article 11 ne porte que sur

[2] Le texte proposé peut être consulté à : https://rm.coe.int/16806b6f7b

[3] Loi réglementant les firmes effectuant des enquêtes sur la solvabilité, publiée au Journal officiel le 15 janvier 2002, qui contient en particulier des dispositions sur la confidentialité, les mesures de sécurité et les droits des 'clients' : http://www.banxico.org.mx/disposiciones/marco-juridico/legislacion-de-interes/leyes/%7B3D04AC1C-8A4B-2331-040C-01A03FDAD3B6%7D.pdf

les « données personnelles contenues dans des bases de données » et recommande de supprimer cette limitation). Le Comité souligne l'exigence prévue à l'article 5 de la Convention 108 que les finalités soient « légitimes », qui devrait être plus clair dans la loi fédérale (et ne pas seulement être prévu dans le cas du traitement de données sensibles). L'article 13 traite de la nécessité d'une finalité limitée et garantit que les données ne sont pas utilisées de manière incompatible avec cette finalité. Cet article inclut également le principe de la limitation des données. Les concepts utilisés ne sont pas toujours définis de la même manière que dans la Convention 108 et il serait utile de mentionner expressément le principe de traitement *loyal* et d'ajouter le concept de finalité *déterminée*, mais on peut constater que, dans l'ensemble, les garanties énoncées par la loi fédérale correspondent à celles de l'article 5 de la Convention 108.

La loi générale qui prévoit les mêmes garanties (voir les articles 16, 18, 19, 23 et 25) et fait, en outre, référence au principe de "loyauté" (article 16) est conforme à l'article 5 de la Convention 108.

Le Comité souligne qu'en ce qui concerne le traitement des données obtenues à partir de sources accessibles au public (article 10(II) de la loi fédérale et article 3(XXV) de la loi générale), des dispositions devraient être prises pour faire en sorte que la nature même des données ne risque pas de porter atteinte aux droits et libertés fondamentales de la personne concernée.

En ce qui concerne la légitimité du traitement des données, l'article 8 de la loi fédérale prévoit que "*sauf dispositions contraires de la présente loi, toutes les opérations de traitement des données à caractère personnel seront assujetties à l'accord du propriétaire des données*", puis définit les caractéristiques du consentement et des autres bases juridiques du traitement des données à caractère personnel (article 10). Le Comité se félicite de cette introduction et note que le fait que le consentement doit être "libre, spécifique et éclairé" est énoncé dans l'article 12 du règlement d'application de la loi fédérale (le projet de Convention 108 modernisé mentionne également le consentement "non équivoque", excluant ainsi la possibilité d'un consentement tacite).

L'article 20 de la loi générale reprend ces prescriptions concernant le consentement dans les situations où il représente la base légale du traitement, tout en prévoyant d'autres fondements légitimes du traitement.

Ces dispositions sont conformes à l'article 5 de la Convention 108.

5. Catégories particulières de données (article 6 de la Convention)

Les catégories particulières de données sont définies à l'article 3 de la loi fédérale et les articles 3(XXVIII) et 21, paragraphe 4 de la loi générale comme indiqué plus haut (voir les définitions).

L'article 9 de la loi fédérale dispose que, "*dans le cas de données à caractère personnel sensibles, la personne chargée de contrôler les données doit obtenir aux fins du traitement le consentement exprès écrit du propriétaire des données, au moyen de la signature faite à la main dudit propriétaire des données, d'une signature électronique ou de tout mécanisme d'authentification créé à cette fin. Les bases de données contenant des données à caractère personnel sensibles ne peuvent pas être créées sans que soit apportée la preuve qu'elles le sont à des fins qui sont légitimes, concrètes et compatibles avec les objectifs poursuivis ou les activités entreprises par la partie soumise à réglementation*."

L'article 7 de la loi générale et l'article 56 du règlement interdisent le traitement des données sensibles sauf lorsque certaines conditions sont réunies.

Toutefois, l'article 7 de la loi générale prévoit que cette interdiction ne s'applique pas dans les cas exposés à l'article 22 de la loi, qui cite une liste de cas où le consentement de la personne

concernée n'est pas exigé. En particulier, l'article 22 (VIII) envisage que le consentement ne soit pas exigé dans des cas où « les données sont contenues dans des sources à accès public ». Il est important de noter que de telles sources peuvent aussi contenir des données sensibles, dont le traitement automatisé pourrait donner lieu à des pratiques discriminatoires ou à d'autres effets adverses pour la personne concernée. Le Comité recommande donc d'élargir l'interdiction du traitement des données sensibles sans le consentement de la personne concernée s'agissant de données contenues dans des sources d'accès public.

Même si les données relatives à la santé sont classées comme données sensibles, la spécificité du traitement de ces données n'est traitée ni dans la loi fédérale ni dans son règlement d'application. Ces aspects sont également absents de la loi générale.

Le Comité préconise d'insérer les modalités applicables au traitement des données relatives à la santé.

6. Sécurité des données (article 7 de la Convention)

L'article 19 de la loi fédérale dispose que "*toutes les parties chargées du traitement des données à caractère personnel doivent établir et pérenniser des mesures de sécurité administrative physiques et techniques destinées à protéger ces données contre l'endommagement, la perte, la modification, la destruction ou l'utilisation, l'accès ou le traitement non autorisés.*
Les personnes chargées du contrôle des données n'adopteront pas de mesures de sécurité inférieures à celles qui leur servent à gérer leurs propres informations. De plus, il sera tenu compte du risque encouru, des conséquences éventuelles pour les propriétaires de données, du caractère sensible des données et de l'évolution technologique." L'article 20 de la loi fédérale introduit le concept de notification au propriétaire des données (c'est-à-dire la personne concernée) des atteintes à la sécurité.

Il convient également de noter les dispositions du chapitre III du règlement d'application de la loi fédérale relatif aux mesures de sécurité à prendre pour le traitement des données à caractère personnel, qui mettent en œuvre une approche de la sécurité des données axée sur les risques (voir en particulier les articles 60 et 61).

La loi générale reprend les prescriptions en matière de sécurité susvisées dans son article 31, et insère une approche de la sécurité des données axée sur les risques dans son article 32 et la notion d'attestation du contrôle de l'application des mesures de sécurité dans ses articles 34 à 36. Cette loi prévoit également l'obligation pour la personne chargée de contrôler les données de notitier toute atteinte à la sécurité à la personne concernée et à l'INAI (article 40).

Les dispositions applicables à la protection des données à caractère personnel (la loi fédérale, le règlement d'application et la loi générale) sont conformes à celles de l'article 7 de la Convention 108. On peut seulement déplorer que la notification de l'atteinte à la sécurité des données à l'autorité de contrôle ne soit pas prévue par la loi fédérale ou son règlement d'application, car cela aurait anticipé pleinement la modernisation de la Convention 108.

7. Garanties complémentaires pour la personne concernée (article 8 de la Convention)

L'article 15 de la loi fédérale dispose que "*la personne chargée de contrôler les données aura l'obligation d'informer les propriétaires des données sur la nature et la raison des informations recueillies sur eux, par le biais de l'avis relatif au respect de la vie privée"* et son article 16 précise les informations à insérer dans l'avis en question. La loi générale contient des prescriptions analogues (articles 26 et 27[4]), qui concordent donc avec les dispositions de l'article 8 de la Convention 108 et avec le principe de transparence inscrit dans le projet de modernisation.

[4] Il convient de noter que, dans la version initiale de la loi, l'article 26 prévoit la dénomination de la personne chargée de contrôler les données, et non pas la dénomination de la personne concernée ("*La dénomination du responsable*").

Le chapitre III de la loi fédérale, en particulier ses articles 22 à 25, garantissent les droits de la personne concernée à l'accès, à la rectification, à l'effacement et à l'objection. Le règlement d'application de la loi fédérale prévoit également un droit de la personne concernée à l'information lorsqu'une décision est prise automatiquement, sans intervention humaine (article 112 du règlement). La loi générale prévoit des prescriptions analogues (articles 43 à 47). L'article 57 de la loi générale institue un droit à la portabilité des données. La loi fédérale et la loi générale sont conformes à l'article 8 de la Convention 108.

De plus, en vertu de l'article 45 de la loi fédérale, le "propriétaire des données" (c'est-à-dire la personne concernée) a le droit de déposer une requête auprès de l'INAI lorsque la demande qu'il a adressée à la personne chargée de contrôler les données n'a pas abouti ou que cette dernière n'y a pas donné suite. Ce droit concorde avec la prescription énoncée dans l'article 8 d de la Convention 108.

Enfin, les personnes concernées peuvent contester une décision de l'INAI et recourir contre elle (voir l'article 56 de la loi fédérale et les articles 138 et 144 de son règlement d'application, et l'article 115 de la loi générale). Cette disposition est conforme à l'article 1, paragraphe 4) du Protocole additionnel, aux termes duquel "(l)es décisions des autorités de contrôle faisant grief peuvent faire l'objet d'un recours juridictionnel".

8. Exceptions et restrictions (article 9 de la Convention)

La loi fédérale limite l'observation des principes et l'exercice des droits établis lorsqu'il s'agit de "protéger la sécurité nationale, l'ordre public, la santé et la sûreté publiques, ainsi que les droits des tiers" (article 4). Le Comité est d'avis qu'une partie des impératifs motivant les restrictions des droits au regard de la loi fédérale pourraient être désignés et définis d'une manière plus restrictive (l'"ordre public", par exemple, étant une notion très générale).

De plus, ni la loi fédérale ni la loi générale ne limitent l'application de certaines dispositions aux opérations de traitement effectuées par la presse dans le cas où ces dispositions aboutiraient à limiter l'exercice de la liberté d'expression..

Le chapitre II de la loi générale, et en particulier son article 80, traite de la collecte et du traitement de données à caractère personnel par les autorités ayant compétence "*dans les domaines de la sécurité, de l'application des lois et l'administration de la justice*" et limite l'application des prescriptions en matière de protection des données dans la mesure où cela est "*nécessaire et proportionné pour leur permettre d'exercer leurs fonctions en ce qui concerne la sécurité nationale, la sûreté publique ou la prévention et la poursuite des infractions*". Un chapitre distinct (Requête en révision sur des questions touchant la sécurité nationale, articles 139 à 143) énonce la procédure de révision touchant les questions de sécurité nationale.

Ces dispositions sont conformes à celles de l'article 9 de la Convention 108.

9. L'autorité de contrôle (article 1 du Protocole additionnel)

La loi fédérale et la loi générale semble établir deux entités différentes chargées de veiller au respect de leurs dispositions respectives.

L'article 38 du chapitre VI de la loi fédérale prévoit l'institution d'une autorité de contrôle appelée "Institut national de la transparence, de l'accès à l'information et de la protection des données à caractère personnel (INAI)", chargée de veiller au respect des mesures donnant effet, dans le droit interne, aux principes énoncés dans la Convention, conformément à l'article 1, paragraphe 1 du Protocole additionnel.

L'article 39 de la même loi décrit en détail les responsabilités de cette autorité de contrôle. L'article 59 mentionne les pouvoirs de vérification, mais non pas expressément ceux "d'investigation et d'intervention" que prévoit l'article 1, paragraphe 1 a du Protocole additionnel. Toutefois, le chapitre IX du règlement d'application de la loi fédérale traite des "inspections" effectuées par l'INAI. La coopération avec les autres autorités de contrôle est prévue à l'article 39 de la loi fédérale et à l'article 89 de la loi générale.

L'article 89 de la loi générale énumère un nombre d'attributions de l'INAI en complément de celles déjà mentionnées, telle que la compétence d'initier des poursuites judiciaires et de se référer aux autorités judiciaires dans le contexte de violations allégées de la protection des données personnelles par une loi nationale (l'article 89 (VIII)). Les Paragraphes (XXXII) et (XXXIII) du même article permettent aussi à l'INAI de soumettre des examens de constitutionnalité contre « la loi fédérale ou locale et tous traités Internationaux signés par le Président de la République et approuvés par le Senat, qui porte atteinte au droit de la protection des données personnelles aussi bien que de promouvoir « *les contestations d'ordre constitutionnel comme prévu par l'article 105, section I, clause I) de la Constitution des Etats-Unis du Mexique* ». La compétence d'initier des recours de constitutionnalité par l'INAI est aussi prévue par l'article 105, fraction II, paragraphe h) de la Constitution.

La composition de l'INAI et les modalités de désignation de ses membres ne sont abordés ni dans la loi fédérale ni dans son règlement d'application. Toutefois, elles le sont dans un document distinct présenté avec la demande d'adhésion à la Convention 108, intitulé "4. Autorité de contrôle du Mexique". Ce document rappelle que l'INAI est doté de pouvoirs en matière de réglementation, d'information, de vérification, de règlement et de sanction. De surcroît, le document renvoie à l'article 6VIII de la Constitution, dont le Comité a eu connaissance et qui précise que l'INAI s'acquitte de sa mission en toute indépendance, est composé de sept commissaires désignés par le Sénat à l'issue d'une large consultation de la société et sur proposition des groupes parlementaires, les candidats devant obtenir les deux tiers des voix des membres présents. Les commissaires sont nommés pour sept ans et élisent leur commissaire en chef au scrutin secret pour une période de trois ans. Certaines prescriptions constitutionnelles garantissent l'absence de conflits d'intérêts.

Par ailleurs, l'article 116 de la Constitution prescrit l'institution au niveau des États fédérés d'organismes autonomes, spécialisés, impartiaux et collégiaux chargés de la protection des données.

L'INAI a mentionné les activités ci-après :

Plaintes générales déposées auprès de l'INAI (2011-2016)	
Reçues	1361
Instruites	1294
En cours d'instruction	72
Procédures de vérification entre juillet 2011 et décembre 2016	**179**
Demandes de protection des droits reçues entre janvier 2012 et décembre 2016	**728**
Dont, fondées	334
Nombre de demandes reçues	**883**
En matière d'accès	381
En matière de rectification	35
En matière d'effacement	310

En matère d'objection	157
Sanctions	
Procédures de sanction engagées	177
Procédures de sanction conclues	113
Demandes concernant le secteur public (parties soumises à obligation) en matière d'accès et de rectification	**296 506**
Recours déposés devant l'INAI contre les réponses aux demandes adressées aux parties soumises à obligation	**1101**
Recommandations, modèles et outils élaborés par l'INAI	
2013	7
2014	6
2015	3
2016	2
2017	3
Formation à la protection des données dispensée par l'INAI	**116**
Nombre total de participants à ces formations	10261

L'article 10 de la loi générale prévoit la mise en place du "Système national de la transparence, de l'accès à l'information et de la protection des données à caractère personnel" (ci-après "le Système national"), qui doit "contribuer à maintenir dans sa plénitude le droit à la protection des données à caractère personnel dans l'ensemble du pays et aux trois niveaux du Gouvernement". Le Système national est réglementé par la loi générale sur la transparence et l'accès à l'information et d'autres lois et règlements qui n'ont pas été mis à la disposition du Comité aux fins du présent examen.

La loi générale mentionne également l'INAI (article 88) et la loi générale sur la transparence et l'accès à l'information, la loi fédérale sur la transparence et l'accès à l'information et d'autres règlements qui "peuvent être applicables". Ces instruments législatifs n'ont pas été mis à la disposition du Comité. La loi générale fait également référence aux "organismes garants" (article 91) sans préciser en quoi ils diffèrent des autres organismes de contrôle existants et mentionnés ni comment la cohérence de leurs compétences respectives est assurée. Il semble que l'Institut national soit l'autorité de contrôle compétente à l'échelon fédéral et que les organismes garants soient compétents à l'échelon des États fédérés, mais cela demeure inexpliqué. En conséquence, le Comité note qu'il conviendrait d'apporter des précisions sur les dispositions de la loi générale relatives au Système national, à l'INAI et aux organismes garants afin d'expliquer clairement la répartition des compétences entre ces divers organismes.

Les articles 146 et 147 portent sur les pouvoirs de contrôle et de vérification de l'Institut et des organismes garants.

Ced dispositions sont conformes à celles de l'article 1 du Protocole additionnel.

10. Sanctions et recours (article 10 de la Convention)

L'article 64 de la loi fédérale prévoit des sanctions administratives visant les violations de la loi fédérale énumérées à l'article 63. Son chapitre XI et, plus particulièrement, ses article 67 à 69 prévoient des sanctions pénales. En particulier, son article 64 prévoit plusieurs sanctions administratives, qui vont du simple avertissement à une amende d'un montant compris entre 100 et 320 000 fois le salaire minimal en vigueur à Mexico. Ces sanctions peuvent être doublées lorsque l'opération de traitement des données visée contient des données sensibles. Les articles 67 à 69 prévoient des sanctions pénales allant de trois mois à cinq années d'emprisonnement, sanctions doublées si des données sensibles sont concernées.

La loi générale institue également des sanctions administratives infligées par l'INAI ou les organismes garants (article 152), qui vont de la mise en demeure publique aux sanctions pécuniaires d'un montant compris entre cent cinquante et mille cinq cents fois la valeur journalière de l'unité de mesure et d'actualisation (article 153).

Les personnes physiques peuvent déposer une plainte auprès de l'autorité de contrôle (article 45 de la loi fédérale) ou saisir la justice. Les parties privées peuvent introduire une demande en annulation des décisions rendues par l'Institut auprès du Tribunal administratif fédéral (article 56). En vertu de la loi générale, "*la personne concernée peut déposer une demande d'examen ou un recours auprès de l'Institut ou des organismes garants, selon le cas, ou encore auprès de l'Unité de transparence*" (article 94). En outre, il peut être fait appel des décisions d'un organisme garant auprès de l'INAI (article 117).

Ces dispositions sont conformes à celles de l'article 10 de la Convention 108.

11. Flux transfrontières de données à caractère personnel (article 12 de la Convention et article 2 de son Protocole additionnel)

Le chapitre V de la loi fédérale porte sur les transferts internationaux et l'article 36 prescrit que le transfert nécessite le consentement de la personne concernée, tandis que l'article 37 dispose ce qui suit :

"*Les transferts nationaux ou internationaux de données peuvent être effectués sans le consentement du propriétaire des données dans les cas suivants :*

I. Lorsque le transfert est prévu par une loi ou un traité auquel le Mexique est partie;

II. Lorsque le transfert est nécessaire à des fins de diagnostic médical ou de prévention médicale, de prestation de soins de santé, de traitement médical ou de gestion des services de santé;

III. Lorsque le transfert est effectué à destination de sociétés holding, de filiales ou sociétés apparentées sous contrôle commun exercé par la personne chargée de contrôler les données, ou d'une société mère ou de toute entreprise appartenant au même groupe que la personne chargée de contrôler les données, agissant dans le cadre des mêmes processus et politiques internes;

IV. Lorsque le transfert est nécessaire aux termes d'un contrat exécuté ou à exécuter dans l'intérêt du propriétaire de données entre la personne chargée de contrôler les données et un tiers;

V. Lorsque le transfert est nécessaire ou prévu par la loi aux fins de la défense de l'intérêt général ou à celles de l'administration de la justice;

VI. Lorsque le transfert est nécessaire à la reconnaissance, à l'exercice ou à la défense d'un droit dans le cadre d'une procédure judiciaire, et

VII. Lorsque le transfert est nécessaire à l'établissement ou au maintien d'un lien juridique entre la personne chargée de contrôler les données et le propriétaire des données."

La section III (article 74) du règlement d'application de la loi fédérale, qui porte sur les transferts internationaux, dispose que "*les transferts internationaux de données à caractère personnel sont possibles lorsque le destinataire de ces données assume les mêmes obligations que la personne chargée de contrôler les données qui transfère les données à caractère personnel*". L'article 76 prévoit en outre la possibilité d'obtenir un avis de l'INAI concernant un transfert international.

De son côté, la loi générale prévoit que "*tous les transferts de données à caractère personnel, qu'ils soient nationaux ou internationaux, sont assujettis à l'accord de la personne concernée*" (article 65) et précise que "*le transfert ou la transmission de données à caractère personnel en dehors du territoire mexicain par la personne chargée de contrôler les données ne peut avoir lieu que si le tiers destinataire ou la personne chargée de traiter les données s'engage à protéger ces données*

dans le respect des principes et des obligations énoncés dans la présente loi et des dispositions applicables en la matière" (article 68).

Le principe de l'adéquation[5] du niveau de protection est énoncé à l'article 65 de la loi générale, lequel fait référence à la protection des données *"dans le respect des principes et des obligations énoncés dans la présente loi".*

La loi fédérale et la loi générale sont toutes deux conformes aux dispositions de l'article 12 de la Convention et de l'article 2 de son Protocole additionnel.

Observations supplémentaires

Le Comité se félicite de l'introduction dans le règlement d'application de la loi fédérale du principe de responsabilité (articles 47 et 48) et d'une approche du traitement des données effectué par la personne chargée de contrôler les données qui est axée sur les risques (article 48, V), anticipant ainsi la modernisation de la Convention 108.

Le Comité accueille également avec satisfaction l'insertion dans la loi générale des notions d'agrément (article 83 du règlement d'application de la loi fédérale) et de droit à la portabilité des données.

Conclusion

Eu égard à ce qui précède, le Comité consultatif estime que le cadre juridique relatif à la protection des données des États-Unis du Mexique satisfait dans l'ensemble aux principes de la Convention 108 et de son Protocole additionnel. Le Comité note que des modifications des dispositions juridiques allant dans le sens des observations contenues dans le présent avis seraient les bienvenues.

Se basant sur l'analyse de la législation applicable en matière de protection des données, le Comité consultatif est d'avis que la demande des États-Unis du Mexique d'être invités à adhérer à la Convention 108 et à son Protocle additionnel devrait être reçue favorablement.

[5] Le principe de l'adéquation, en vertu duquel "le transfert de données à caractère personnel vers un destinataire soumis à la juridiction d'un État ou d'une organisation qui n'est pas Partie à la Convention [peut être effectué uniquement] si cet État ou cette organisation assure un niveau de protection adéquat pour le transfert considéré" et, "par dérogation, si le droit interne le prévoit pour des intérêts spécifiques de la personne concernée, ou lorsque des intérêts légitimes prévalent, en particulier des intérêts publics importants, ou si des garanties pouvant notamment résulter de clauses contractuelles sont fournies par la personne responsable du transfert et sont jugées suffisantes par les autorités compétentes, conformément au droit interne" est garanti à l'article 2 du Protocole additionnel.