COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 18 October / octobre 2017 T-PD(2017)07Bil

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

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

(T-PD)

COMPILATION OF OPINIONS / COMPILATION DES AVIS

Directorate General of Human Rights and the Rule of Law /

Direction Générale droits de l'Homme et Etat de droit

TABLE DES MATIERES

OPINION ON THE REQUEST FOR ACCESSION BY ARGENTINA

(T-PD(2017)12)

Introduction

On 29 May 2017 the Secretary General of the Council of Europe received a letter dated 15 May 2017 informing him that the Republic of Argentina wished to accede to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter, "Convention 108").

The Consultative Committee of Convention 108 would point out that, in 2008, it referred to the Committee of Ministers its recommendation for non-member states with data protection legislation in compliance with Convention 108 to be invited to accede to the Convention. The Ministers' Deputies took note of this recommendation and agreed to examine every accession request in the light of it (1031st meeting, 2 July 2008).

Opinion

In accordance with Article 4 of Convention 108, each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in the Convention (Chapter II).

Having taken note of the Argentinian Constitution (Article 43.3) and having examined[1] the *Personal Data Protection Act* of 4 October 2000, hereinafter "the Act", the Committee notes the following.

Lastly, the Consultative Committee furthermore underlines that, following an opinion of the Article 29 Working Party,[2] the European Commission adopted a decision[3] recognising the adequacy of measures taken by Argentina in respect of protection for personal data.

1. Object and purpose (Article 1 of Convention 108)

Section 1 of the Act states that its purpose is the "*comprehensive protection of personal information recorded in files, records, databases, databanks or other technical means of data processing, either public or private for purposes of providing reports, in order to guarantee the right of individuals to their honour and privacy, as well as access to the recorded information"*. The spirit of this section is the same as that of Convention 108, noting the broad interpretation given by the competent bodies (supervisory authority and courts) to the notion of "providing reports" and the fact that this criterion doesn't imply a reduction of the scope of the Act. Furthermore, Article 1 of Convention 108 which aims to secure for every individual "respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection")" protects individuals with respect to the processing of any information relating to them, not only data relating to their private life.

Section 1 of the Act also refers to Article 43.3 of the Argentinian Constitution which provides that any individual may bring a "*habeas data"* action (a special judicial remedy with regard to personal data protection, whereby any individual is entitled to access data pertaining to him or her, and to request the deletion or rectification of such data if they are inaccurate or used for discriminatory purposes).

The Act has a total of 46 sections. Under Section 45 of the Act the Executive is required to adopt implementing regulations and establish appropriate supervisory bodies within 180 days of its promulgation. The provinces are encouraged to accede to the provisions of the Act. Federal jurisdiction applies in respect of data registers, files, or banks interconnected via international networks (Section 44).

[1] On the basis of an unofficial English translation of the Act.
The Committee also took note of Decree No. 1558/2001 but was not able to take it into account in its analysis.
[2] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp63_en.pdf
[3] Decision of the Commission.pdf

2. Definitions

Section 2 of the Act lays down definitions for "personal data", "sensitive data", "data owner" (data subject) "data user" (controller), "data dissociation" ("*treatment of personal data in such a way that information obtained cannot be related to any certain or ascertainable person"*).

A. Personal data (Article 2.a of the Convention)

The Act defines "personal data" as *"information of any kind pertaining to certain or ascertainable physical persons or legal entities"*.

The Act furthermore defines "data owners [subjects]" as *"any physical person or legal entity having a legal domicile or local offices or branches in the country, whose data are subject to the treatment [processing] referred to in this Act".*

Although it also covers legal persons (a possibility available to Parties to the Convention) this definition corresponds to the one given in Article 2.a of Convention 108, the domicile condition only being applicable to legal persons.

B. Special categories of data (Article 6 of the Convention)

"Sensitive data" are defined in the Act as "(*p)ersonal data revealing racial and ethnic origin, political opinions, religious, philosophical or moral beliefs, trade union membership, and information concerning health conditions or sexual habits or behaviour*."

The Committee notes that although the definition of sensitive data makes no reference to data relating to criminal convictions, such data are covered under separate provisions of the Act (Section 7.4 and, concerning data processed by the police, Section 23.3).

C. Automatic processing (Article 2.c of the Convention)

The Act mentions different data files, both public and private (Sections 22, 24, 27, 28), as well as public and private data file registers (Section 21). It defines data subject to processing and the registers in which such data are kept and defines data processing as "*(s)ystematic operations and procedures, either electronic or otherwise, that enable the collection, preservation, organisation, storage, modification, relation, evaluation, blocking, destruction, and in general, the processing of personal information, as well as its communication to third parties through reports, inquiries, interconnections or transfers*."

Although not confined to automatic processing, the definition of data processing pursuant to the Act is compatible with Article 2.c of the Convention. Indeed, it may be desirable to apply the Act even in cases where there is no automatic processing when the processing in question involves operations carried out on personal data within a structured set of data which are accessible or may be found using specific criteria or which enable the controller or anyone else to search for, combine or correlate data pertaining to a given individual.

D. Controller of the file (Article 2.d of the Convention)

The Act defines the "data user" as "(*a)ny person, either public or private, performing in its, his or her discretion the treatment of data contained in data files, registers, databases or databanks, owned by such persons or to which they may have access through a connection."* This definition corresponds to the definition given under Article 2.d of Convention 108.

3. Scope of the data protection regime (Article 3 of the Convention)

The Act applies to the processing of personal data contained in, or for inclusion in, files, registers, bases, banks, where the data user (controller) is on Argentinian territory, and whether such processing concerns the public or private sector. This scope is apparent from the definitions of data user (controller) (Section 2) and other sections of the Act which refer to both sectors (for example Section 21 applies to "(a)ny public or private data file", and Section 35 states that action may be brought against "public or private data bank users").

Under Section 1.1 of the Act "*(i)n no case shall journalistic information sources or data bases be affected*." The Committee notes that a regime of specific exceptions would be preferable.

Lastly, although Section 28 states that the Act does not apply to opinion polls, surveys and statistics, it also provides that a data dissociation technique must be used in cases where it is impossible to ensure anonymity. The Committee notes that such data, as long as they are not made anonymous, are personal data which should thus be covered by the Act.
This scope corresponds to the scope defined in Article 3 of Convention 108. However, the Committee is of the opinion that a general provision defining the scope of the Act would add greater clarity to the text.

4. Quality of data (Article 5 of the Convention)

Processing of personal data cannot be carried out without the consent of the data subject or must fulfil one of the five conditions set out under Section 5.2 of the Act. These principles and bases for determining the lawfulness of personal data processing are legitimate and comply with the provisions of Article 5 of the Convention. Nonetheless, the Committee emphasises that with respect to the processing of data that are clearly in the public domain (Section 5.2a), steps should be taken to make sure that the very nature of the data does not risk infringing the data subject's rights and fundamental freedoms and to restrict this principle to data made public by the data subject.

Personal data collected for processing purposes must be "certain, appropriate, pertinent and not excessive with reference to the scope within and purpose for which such data were secured" (Section 4.1); data must not be collected using disloyal or fraudulent means (Section 4.2); data must not be used for any purposes other than or incompatible with the purposes for which they were collected (Section 4.3); and data must be accurate and up-to-date (Section 4.4); inaccurate or incomplete data must be deleted or replaced (Section 4.5).

These provisions of the Act comply with Article 5 of Convention 108.

5. Special categories of data (Article 6 of the Convention)

Section 7 of the Act protects sensitive data. No one may be forced to communicate sensitive data (Section 7.1); such data may only be collected and processed in circumstances that are in the general interest and permitted by law, or for statistical or scientific purposes, and providing the data subjects cannot be identified (Section 7.2); it is forbidden to create files, banks or registers which reveal sensitive data, whether directly or indirectly (Section 7.3); data pertaining to criminal convictions may only be processed by the competent public authorities (Section 7.4). Special conditions applicable to the processing of health-related personal data are set out in Section 8 of the Act.

The relevant provisions of the Argentinian Act comply with the protection rules laid down in Article 6 of Convention 108.

6. Data security (Article 7 of the Convention)

Under Section 9 of the Act, the controller must take such technical and organisational measures as are necessary to guarantee the security and confidentiality of the personal data, in order to prevent their alteration, loss, unauthorised consultation or processing, and to allow for the detection of any intentional or unintentional distortion of such information, whether such risks stem from human conduct or the technical means used. Furthermore, Section 10 emphasises the controller's duty of professional secrecy (Section 10.1), which may only be lifted by means of legal action or on national defence, or public health and safety grounds (Section 10.2).

The relevant provisions of the Argentinian Act comply with Article 7 of Convention 108.

7. Additional safeguards for the data subject (Article 8 of the Convention)

Under Section 6 of the Act, every time personal data are collected the data subject must be expressly informed in advance and in a clear manner of the purpose of the files, of their existence, of the compulsory or discretionary nature of the questions asked, of the consequences of supplying or refusing to supply the data, and of the right to access, rectify or delete the data. Furthermore, Section 13 of the Act provides "*(a)ny person may request information from the competent controlling Agency regarding the existence of data files, registers, bases or banks containing personal data, their purposes and the identity of the persons responsible therefor. The register kept for such purpose may be publicly consulted, free of charge*." Lastly, Section 15 describes the quality of the substance of information that must be provided to data subjects.

The Committee is nonetheless unsure as to the exact scope of Section 13 of the Act given that Section 41, which also concerns the right to information, no longer refers to the "controlling Agency" but only to the data file, register or bank. Section 41 also stipulates that the reply given to the information request must state the reasons for providing or not providing the requested information.

Sections 14 and 15 establish a right of access. The right to rectify, update or delete data is established under Section 16.

Section 42 establishes the right to request the deletion, rectification and updating of data within three days of the answer given to the information request.

Section 29 provides for the creation of a supervisory authority overseeing data protection. This supervisory authority is responsible for taking all necessary steps to ensure compliance with the aims and provisions of the Act. To that end, it performs a number of different functions, including assisting and advising the data subject, in particular with regard to his or her rights as set out above.

Activity reported of the supervisory authority is as follows:

Current Open Case Files (investigations)	821
Do Not Call Complaints	375
Other general Complaints	446
Advice (2016 -today)	51,789
Do Not Call (by email, tel. or personally at the office)	49,729
For possible other complaints (same)	2,060
Sanctions	236
Do Not Call law	93
Other cases (law 25.326)	143
Rules issued by the authority ("Disposiciones")	49
Rules on Registration	18
Rules on Sanctions Regime	6
Special Rules interpreting the law	9
Rules related to Inspections	5
Rules on Good Practices	3
Rules on the Internal Organisation of the authority	5
Rules interpreting Do Not Call regime	3
Data Bases Registered	64,434
Private Data Bases	33,325
Public Data Bases	262
Others	30847
Inspections (2008-today)	496
Year 2008	4

Year 2009	16
Year 2010	47
Year 2011	28
Year 2012	40
Year 2013	59
Year 2014	67
Year 2015	110
Year 2016	97
Year 2017	28

The Committee notes that the Article 29 Working Party underlined the necessity to reinforce the independence of the supervisory authority and stands ready to assist Argentinian authorities in that respect.

These Sections of the Act comply with the provisions of Article 8 of the Convention.

8. Exceptions and restrictions (Article 9 of the Convention)

There are no unconditional exceptions under the Argentinian Act, only limited derogations and restrictions.

Section 23.2 of the Act provides that "*processing of personal data by the armed forces, security forces, police or intelligence services for national defence or public safety purposes, without the consent of the parties concerned, shall be limited to the cases and data categories strictly necessary for fulfilment of these organisations' statutory obligations with regard to national defence, public safety or law-enforcement. In such cases, files must be specific, drawn up for that particular purpose, and categorised according to their reliability*."

Furthermore, Section 17 of the Act provides for exceptions to the right of access, rectification and deletion (Section 17.1) and the right of information (Section 17.2) in the case of public databanks. Such rights may be denied when they may affect legal or administrative proceedings in cases concerning tax or social security obligations, criminal investigations or the carrying out of environmental and health checks. Furthermore, Section 40 provides that when an exception is made under Section 17 the controller must prove that the situation falls within the scope of Section 17.

Section 40 of the Act provides that in the event of a judicial action the confidentiality obligation incumbent on controllers operating in the private sector still applies with regard to journalistic sources.

The relevant provisions of the Argentinian Act comply with Article 9 of Convention 108.

9. Sanctions and remedies (Article 10 of the Convention)

Data files are deemed to have been duly registered when the principles set out in the Act and in regulations deriving from the Act are respected (Section 3). Moreover, the purpose of data files must not be unlawful (Section 3). Accordingly, the Argentinian Act provides for administrative sanctions under Section 31 and criminal sanctions under Sections 32 to 43 in the event of failure to abide by the law. A breach of confidentiality or data security is a violation of personal databanks (Section 32). Section 33 defines the legal remedies available for the protection of personal data or "*habeas data*". Sections 34 to 39 set out the details regarding legal action, who is entitled to take action, the parties against whom proceedings may be brought, competent jurisdiction, the applicable procedure, and the conditions that must be met.

The provisions of the first four chapters (general provisions, general data protection principles, rights of the data subject, controllers) and Section 32 (criminal sanctions) are public order provisions (Section 44.1).

The Act complies with Article 10 of Convention 108.

10. Transborder flows of personal data (Article 12 of the Convention)

Section 12 of the Act concerns international transfers and provides that transfers of any kind of personal information to States or international organisations that fail to provide an adequate level of protection are prohibited (Section 12.1), subject to the following exceptions: international judicial cooperation, international treaties, international police cooperation in the fight against organised crime or terrorism, and the exchange of medical data or stock exchange or banking transfers (Section 12.2).

Section 12 of the Act meets the requirements of Article 12 of Convention 108.

Additional comments

The Committee very much welcomes Section 20 of the Act concerning objections to personal assessments, which stresses that judicial or administrative decisions must not be based solely on electronic processing of personal data. These provisions, which are in line with the modernised Convention (Article 8.a), would need to be extended so that they also cover processing by the private sector.

Moreover, whereas Sections 25 and 26 of the Act, which concern the supply of IT services and information services, go some way to defining what a processor is, an express future reference to such a processor would be a good thing (as will be the case, for example, in the modernised Convention).

Furthermore, the Committee notes that it would also be worthwhile including a right to object in the Act, as well as a definition of data recipients.

Lastly, the Committee welcomes the fact that the Act contains a Section on direct marketing (Section 27.1).

Although the request made by Argentina only concerns accession to the Convention, the Committee would emphasise that for data protection to be effective it is important to set up a data protection authority, such as that established under Section 29 of the Act, in accordance with Article 1 of the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (hereinafter “Additional Protocol”). Section 29 of the Act provides for the establishment of a supervisory body (“Controlling Agency”) with authority to take all necessary steps to ensure compliance with the aims and provisions of the Act. While its functions and powers are defined under Section 29, the Act also ought to provide a clear definition of its status, composition, and budget, as well as the remit of its members and how they are appointed.

Lastly, the Committee welcomes Section 30 of the Act which provides that bodies representing controllers may adopt professional codes of conduct with a view to guaranteeing and improving the conditions of operation of information systems. Such codes are to be registered with the supervisory body, which may refuse registration if it considers that a code fails to comply with the law.

Conclusion

In light of the above, the Consultative Committee considers that the Argentinian Act on data protection is in full compliance with the provisions of Convention 108. Accordingly, based on its analysis of the applicable data protection legislation, the Consultative Committee is of the opinion that the request from Argentina to be invited to accede to Convention 108 should be given a favourable response.

The Committee further recommends that the Republic of Argentina be invited to accede to the additional Protocol.

26 June 2017

AVIS SUR AVIS SUR LA DEMANDE D'ADHÉSION DE L'ARGENTINE

Introduction

Le 29 mai 2017, le Secrétaire Général du Conseil de l'Europe a reçu une lettre datée du 15 mai 2017, lui faisant part du souhait de la République d'Argentine d'adhérer à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ci-après, la « Convention 108 »).

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 Etats 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).

Après avoir pris note de la Constitution de la Nation argentine (article 43.3) et avoir examiné[4] la loi du 4 octobre 2000 *sur la protection des données personnelles* de l'Argentine, ci-après désignée « la loi », le Comité constate ce qui suit.

Le Comité consultatif souligne par ailleurs que la Commission européenne, suite à l'avis rendu par le Groupe de travail de l'article 29[5], a pris le 2 juillet 2003 une décision[6] reconnaissant l'adéquation des mesures prises par l'Argentine en matière de protection des données à caractères personnel.

11. Objet et but (article1er de la Convention 108)

L'article 1er de la loi énonce son objet : *« protéger intégralement les données personnelles consignées dans des fichiers, des registres, des banques de données ou d'autres moyens techniques de traitement des données, publics ou privés, destinés à fournir des informations, cela afin de garantir le droit des personnes à leur honneur et à leur vie privée, ainsi que l'accès à l'information enregistrée* ». Si l'article 1er de la loi sur la protection des données s'inscrit dans l'esprit de la Convention 108, il convient de noter l'interprétation large par les instances compétentes (autorité de contrôle, tribunaux) de la notion '*fournir des informations*' et du fait que cette précision n'a pas pour effet de réduire le champ d'application de la loi. Par ailleurs, l'article 1er de la Convention 108, qui vise à garantir à toute personne physique « le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant (« protection des données ») » permet quant à lui de protéger une personne au regard du traitement de données personnelles autres que celles purement relatives à sa vie privée.

L'article 1er de la loi fait par ailleurs référence à l'article 43. 3 de la Constitution argentine qui prévoit que toute personne peut avoir recours à « l'*habeas data* » (recours juridictionnel spécial en matière de protection des données personnelles permettant à toute personne d'accéder aux données la concernant, d'en demander la suppression ou la correction en cas d'inexactitude ou d'utilisation à des fins discriminatoires).
La loi est composée de 46 articles ; son article 45 prévoit l'adoption par le pouvoir exécutif de règlements d'application ainsi que la création des organes de contrôle idoines dans les 180 jours suivant la promulgation.

[4] Sur la base d'une traduction non-officielle en anglais de la loi. Les extraits reproduits dans le présent avis ont été traduits en français par le Secrétariat du Comité, qui ne saurait en être tenu responsable.
Le Comité a par ailleurs pris note du décret No. 1558/2001 sans toutefois avoir été en mesure d'en tenir compte dans son analyse).
[5] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp63_fr.pdf
[6] http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1415636698083&uri=CELEX:32003D0490

Les provinces sont encouragées à adopter la loi ; la compétence fédérale s'applique à l'égard des registres de données, des fichiers ou des banques interconnectés par le biais de réseaux internationaux (art. 44).

12. Définitions

Dans son article 2, la loi énonce les définitions des « données personnelles », des « données sensibles », du « titulaire des données » (personne concernée), de « l'utilisateur de données » (responsable du traitement), de la « dissociation des données » (*« traitement des données à caractère personnel de telle sorte que les informations obtenues ne puissent être liées à une personne déterminée ou déterminable »*).

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

La loi définit les « données personnelles », comme des *« informations de toute nature concernant les personnes physiques ou morales déterminées ou déterminables »*.

La loi définit par ailleurs les personnes concernées comme étant « *toute personne physique ou morale ayant son domicile légal, ses locaux ou des succursales dans le pays, dont les données sont soumises au traitement visé* » dans la loi.

Cette définition, tout en visant également les personnes morales (possibilité laissée aux Parties à la Convention) correspond à celle donnée par l'article 2.a de la Convention 108, étant établi que la condition liée à la domiciliation n'est pas applicable aux personnes physiques.

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

Les « données sensibles », à savoir : les *« données personnelles révélant l'origine raciale et ethnique, les opinions politiques, les croyances religieuses, philosophiques ou morales, l'affiliation syndicale et les informations concernant l'état de santé ou la vie sexuelle »*.

Le Comité note que la définition des données sensibles ne mentionne pas les données concernant les données relatives aux condamnations pénales, ces données font néanmoins l'objet de dispositions spécifiques (art. 23.3, ainsi que s'agissant des données traitées par la police, art. 7.4).

G. Traitement automatisé (article 2.c de la Convention)

La loi mentionne différents fichiers de données, publics ou privés (art. 22, 24, 27, 28), ainsi que les registres des fichiers de données, publics ou privés (art. 21). La loi définit les données sujettes au traitement ainsi que les registres dans lesquels celles-ci sont conservées et elle définit le traitement de données comme étant les « *opérations et procédures systématiques, par voie électronique ou autre, permettant la collecte, la conservation, le stockage, la modification, la relation, l'évaluation, le blocage, la destruction, et, de façon générale, le traitement des informations à caractère personnel, ainsi que leur cession à des tiers par voie de communication, de consultation, d'interconnexion ou de transfert* ».

La définition du traitement des données prévue par la loi tout en ne se limitant pas au caractère automatisé du traitement est compatible avec l'article 2.c de la Convention. En effet, il peut être souhaitable d'assurer une application de la loi quand bien même aucun procédé automatisé ne serait utilisé dès lors que le traitement de données concerné vise des opérations effectuées sur des données à caractère personnel au sein d'un ensemble structuré de données qui sont accessibles ou peuvent être retrouvées selon des critères spécifiques ou qui permettent au responsable du traitement ou à toute autre personne de rechercher, combiner ou mettre en corrélation des données relatives à une personne.

H. Responsable du traitement/maître du fichier (article 2.d de la Convention)

La loi définit « l'utilisateur de données » comme *« toute personne, publique ou privée, exerçant, à sa discrétion, le traitement de données qu'elles soient dans des fichiers, registres ou banques de données appartenant à ces personnes ou dont elles disposent par connexion* ». Cette définition correspond à celle donnée par l'article 2.d de la Convention 108.

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

La loi s'applique aux traitements de données personnelles contenues ou appelées à figurer dans les fichiers, registres, bases, banques, dont l'utilisateur (le responsable du traitement) se trouve sur le territoire de l'Argentine, que ce traitement relève du secteur public ou privé, tel que cela ressort des définitions du responsable de traitement (art. 2) et d'autres articles de la loi qui font référence à ces deux secteurs (l'article 21 vise par exemple « tout fichier de données, public ou privé », et l'article 35 énonce qu'une action est possible contre « des banques de données publiques ou privées »).

L'article 1.1 de la loi dispose que « *les sources d'information ou les bases de données des journalistes ne doivent en aucun cas être affectées* ». Le Comité note qu'un régime de dérogations spécifiques serait préférable.

Enfin, l'article 28 exclut du champ d'application de la loi les sondages, les études et les statistiques, il assure cependant des garanties, en énonçant qu'une dissociation des données doit être effectuée dans le cas où une anonymisation ne serait pas possible. Le Comité note que ces données, tant qu'elles ne sont pas rendues anonymes, sont des données personnelles qui devraient à ce titre être couvertes par la loi.

Ce champ d'application correspond à celui énoncé à l'article 3 de la Convention 108. Le Comité est cependant d'avis qu'une disposition générale quant au champ d'application de la loi ferait gagner en clarté au texte.

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

Le traitement des données personnelles doit avoir reçu le consentement de la personne concernée ou répondre à l'une des cinq conditions prévues par l'article 5.2 de la loi. Ces bases de licéité du traitement et fondements sont légitimes et sont conformes aux dispositions de l'article 5 de la Convention. Néanmoins, le Comité souligne que s'agissant du traitement des données rendues manifestement publiques (art. 5.2.a), il conviendrait de veiller à ce que la nature même de ces données ne soient pas susceptibles de constituer un risque d'atteinte aux droits et libertés fondamentales de la personne concernée, et de limiter ce fondement aux seules données rendues publiques par la personne concernée elle-même.

Les données à caractère personnel recueillies à des fins de traitement doivent être certaines, appropriées, pertinentes et non excessives eu égard à la portée ou à la finalité pour lesquels elles ont été obtenues (art. 4.1) ; la collecte des données ne doit pas être effectuée par des moyens déloyaux ou frauduleux ni d'une manière contraire à la loi (art. 4.2) ; les données ne doivent pas être utilisées à des fins différentes ou incompatibles de celles qui ont donné lieu à leur collecte (art. 4.3) ; les données doivent être exactes et actualisées (art. 4.4) ; les données inexactes ou incomplètes doivent être supprimées ou remplacées (art. 4.5).

Les dispositions de la loi sont conformes à celles de l'article 5 de la Convention 108.

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

L'article 7 de la loi protège les données sensibles : personne ne peut être contraint à communiquer des données sensibles (art. 7.1) ; celles-ci ne peuvent être collectées et traitées que s'il existe des circonstances d'intérêt général autorisées par la loi, ou à des fins statistiques ou scientifiques, et à condition que les personnes concernées ne puissent être identifiées (art. 7.2) ; il est interdit de créer des fichiers, banques ou registres révélant directement ou indirectement des données sensibles (art. 7.3). Les données relatives aux condamnations pénales ne peuvent être traitées que par les autorités publiques compétentes (art. 7.4). La particularité du traitement des données à caractère personnel dans le domaine de la santé est prévue à l'article 8 de la loi.

En ses dispositions pertinentes, la loi argentine correspond au régime de protection établi par l'article 6 de la Convention 108.

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

Selon l'article 9 de la loi, le responsable du traitement doit prendre les mesures techniques et organisationnelles nécessaires pour garantir la sécurité et la confidentialité des données personnelles, afin d'éviter leur altération, leur perte, leur consultation ou leur traitement non autorisés, ainsi que pour permettre de détecter toute altération intentionnelle ou non intentionnelle de ces informations, que le risque découle d'une action humaine ou des moyens techniques utilisés. L'article 10 souligne par ailleurs le devoir de secret professionnel qui incombe au responsable du traitement (art.10.1), l'obligation de confidentialité ne pouvant être levée que par voie judiciaire ou pour des motifs de défense nationale, de sécurité et de santé publiques (art.10.2).

En ses dispositions pertinentes, la loi argentine est conforme à l'article 7 de la Convention 108.

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

L'article 6 de la loi dispose que chaque fois que des données personnelles sont recueillies, la personne concernée doit être préalablement informée de manière explicite et claire du but, de l'existence des fichiers, de la nature obligatoire ou discrétionnaire des questions posées, des conséquences de la communication des données ou du refus de les fournir, de la possibilité d'exercer les droit d'accès et de rectification ou de suppression. Par ailleurs la loi prévoit dans son article 13 que *« toute personne peut demander au responsable du traitement des informations sur l'existence de fichiers de données, de registres, de bases ou de banques contenant des données à caractère personnel, leurs finalités et l'identité des personnes responsables. Le registre tenu à cette fin peut être consulté publiquement sans frais »*. L'article 15 précise enfin la qualité du contenu de l'information à fournir aux personnes concernées.

Le Comité s'interroge néanmoins sur la portée exacte de l'article 13 en raison du fait que l'article 41 de la loi, également relatif au droit d'information ne fait plus référence au « responsable du traitement » mais seulement « aux fichiers, registres ou banques de données ». Cet article énonce également que dans la réponse à la demande d'information, les raisons pour lesquelles les informations demandées sont communiquées ou pour lesquelles la demande n'aboutit pas, doivent être explicitées.

Les articles 14 et 15 prévoient un droit d'accès ; les droits de rectification, de mise à jour ou de suppression sont précisés à l'article 16.

L'article 42 énonce un droit de demande de suppression, correction et de mise à jour de la donnée dans les trois jours suivants la réponse à la demande d'information.

L'article 29 prévoit la création d'une autorité de contrôle de la protection des données. Cette autorité est chargée de prendre toutes les mesures nécessaires au respect des objectifs et des dispositions de la loi. Elle exerce à cette fin différentes fonctions, au nombre desquelles l'assistance et le conseil de la personne concernée, notamment dans l'exercice des droits susmentionnés.

L'activité de l'autorité de contrôle est présentée comme suit :

Dossiers en cours d'examen	821
Plaintes « Do Not Call »	375
Autres plaintes générales	446
Conseils (à partir de 2016)	51,789
"Do Not Call" (par email, tel. ou en personne à l'autorité)	49,729
Au sujet d'autres plaints possibles	2,060
Sanctions	236
Loi « Do Not Call »	93
Autres cas (loi 25.326)	143
Avis prononcés par l'autorité ("Disposiciones")	49
Sur l'enregistrement	18

Sur le régime de sanction	6
Sur l'interprétation de la loi	9
Sur les contrôles	5
Sur les bonnes pratiques	3
Sur l'organisation interne de l'autorité	5
Sur le régime "Do Not Call"	3
Bases de données enregistrées	64,434
Secteur privé	33,325
Secteur public	262
autres	30847
Contrôles (depuis 2008)	496
Année 2008	4
Année 2009	16
Année 2010	47
Année 2011	28
Année 2012	40
Année 2013	59
Année 2014	67
Année 2015	110
Année 2016	97
Année 2017	28

Le Comité note que la nécessité de renforcer l'indépendance de cette autorité avait été soulignée par le Groupe de l'Article 29.

Ces articles sont conformes aux dispositions de l'article 8 de la Convention.

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

La loi argentine ne prévoit aucune exception inconditionnelle mais uniquement des dérogations et des restrictions limitées.

L'article 23.2 de la loi dispose notamment que *« le traitement des données personnelles à des fins de défense nationale ou de sécurité publique par les forces armées, les forces de sécurité, la police ou les services de renseignements, sans le consentement des parties concernées, est limité aux cas et catégories de données nécessaires pour la stricte mise en œuvre des obligations légalement confiées à ces organismes pour la défense nationale, la sécurité publique ou la répression des infractions. Dans ces cas, les dossiers doivent être spécifiques, établis à cette fin, et ils doivent être classés par catégories selon leur degré de fiabilité »*.

L'article 17 de la loi établit par ailleurs des exceptions en matière de droits d'accès, de rectification ou de suppression (art.17.1) et en matière de droit d'information (art.17.2) lorsqu'il s'agit de banques de données publiques, ces droits peuvent en effet être refusés lorsque ceux-ci peuvent avoir une incidence sur des poursuites judiciaires ou administratives relatives aux obligations fiscales ou liées à la sécurité sociale, une enquête pénale ou encore sur l'effectivité des fonctions de contrôle sanitaire ou écologique. Par ailleurs, en vertu de l'article 40, quand une exception relevant de l'article 17 est soulevée, le responsable doit apporter la preuve que la situation entre dans le cadre de ces exceptions.

L'article 40 de la loi dispose que dans le cas d'un recours juridictionnel, l'obligation de confidentialité incombant au responsable du traitement relevant du secteur privé est maintenue en ce qui concerne les sources journalistiques.

Les dispositions pertinentes de la loi argentine sont conformes à l'article 9 de la Convention 108.

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

Les fichiers de données sont dûment enregistrés lorsque les principes énoncés par cette loi ainsi que par les textes réglementaires en découlant sont respectés (art. 3). De plus, les fichiers de données ne doivent pas avoir d'objet contraire aux lois (art. 3). En conséquence, la loi argentine prévoit des sanctions administratives à l'article 31 et des sanctions pénales aux articles 32 à 43 en cas de non-respect de la loi. Porter atteinte à la confidentialité ou à la sécurité des données constitue une violation des banques de données personnelles (art. 32). L'article 33 expose les voies de recours « pour la protection des données, ou « *habeas data* ». Les articles 34 à 39 détaillent cette action, les personnes habilitées à l'engager, celles contre lesquelles elle peut être engagée, la juridiction compétente, la procédure à suivre ainsi que les conditions que celle-ci doit remplir.

Les dispositions des quatre premiers chapitres (dispositions générales, principes généraux en matière de protection des données, droits de la personne concernée, responsables du traitement) ainsi que l'article 32 (sanctions pénales) sont d'ordre public (art. 44.1).

La loi satisfait à l'article 10 de la Convention 108.

20. Flux transfrontières de données à caractère personnel (article 12 de la Convention)

L'article 12 de loi porte sur les transferts internationaux. Il dispose que le transfert de tout type de renseignements personnels à des Etats ou à des Organisations internationales ne fournissant pas un niveau adéquat de protection, est interdit (art. 12.1), sauf exceptions suivantes : coopération judiciaire internationale, traités internationaux, coopération policière internationale dans la lutte contre la criminalité organisée ou le terrorisme et échange d'informations médicales ou transferts bancaires et boursiers (art. 12.2).

L'article 12 de la loi est conforme aux exigences de l'article 12 de la Convention 108.

Remarques complémentaires

Le Comité salue vivement l'article 20 de la loi portant sur l'objection aux évaluations personnelles, celui-ci souligne en effet que les décisions judiciaires ou administratives ne doivent pas avoir pour seule base le traitement informatisé de données personnelles. Ces dispositions qui vont dans le sens de la Convention modernisée (art.8.a) nécessiteraient d'être étendues aux traitements réalisés par le secteur privé.

En outre, les articles 25 et 26 de la loi, portant respectivement sur la fourniture de services informatiques et d'information, amorcent une définition de la sous-traitance, qu'il serait utile de prévoir expressément à l'avenir (tel que ce sera notamment le cas dans le cadre de la modernisation de la Convention).

Par ailleurs, le Comité note qu'il serait également opportun d'introduire dans la loi un droit d'opposition et une définition du destinataire.

Le Comité salue enfin l'existence dans la loi d'un article dédié spécifiquement au marketing direct (art. 27.1).

Bien que la demande de l'Argentine ne porte que sur l'adhésion à la Convention, le Comité souligne l'importance pour l'effectivité de la protection des données de l'établissement d'une autorité de protection des données, telle que celle établie par l'article 29 de la loi et conformément à l'article 1 du Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données (ci-après « Protocole additionnel »). L'article 29 de la loi prévoit en effet qu'une autorité de contrôle, habilitée à prendre toutes les mesures nécessaires pour se conformer aux objectifs et aux dispositions de la loi soit établie. Si ses fonctions et ses pouvoirs sont précisés, il conviendrait également de définir clairement dans la loi son statut, sa composition, son budget ainsi que le mandat et la nomination de ses membres.

Le Comité salue enfin l'article 30 de la loi qui prévoit que les organismes représentant les responsables du traitement peuvent adopter des codes de conduite professionnelle aux fins d'assurer et d'améliorer les conditions de fonctionnement des systèmes d'information ; ces codes sont inscrits au registre tenu par l'autorité de contrôle, qui peut en refuser l'enregistrement au cas où elle estimerait que lesdits codes ne sont pas conformes à la loi.

Conclusion

Eu égard à ce qui précède, le Comité consultatif estime que la loi de l'Argentine sur la protection des données satisfait pleinement aux dispositions de la Convention 108. Aussi le Comité consultatif, se basant sur l'analyse de la législation applicable en matière de protection des données, est d'avis que la demande de l'Argentine d'être invitée à adhérer à la Convention 108 devrait être reçue favorablement.

Le Comité recommande par ailleurs que la République d'Argentine soit également invitée à adhérer au Protocole additionnel.

OPINION ON THE MSI-NET DRAFT RECOMMENDATION

"Guidelines on the protection and promotion of human rights and fundamental freedoms with regard to internet intermediaries"

1. The Steering Committee on Media and Information Society (CDMSI) invited on 7 July 2017 the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) to provide comments on the draft Recommendation prepared by the Committee of Experts on Internet Intermediaries (MSI-NET).

2. Considering the fact that this consultation falls within the summer period, the Plenary Committee of Convention 108 is not in a position to adopt an opinion on the draft Recommendation and the comments provided hereafter have thus been prepared by its Bureau.

3. The Bureau of the Committee of Convention 108 welcomes this important work and emphasises the necessity of developing guidelines on the protection and promotion of human rights and fundamental freedoms with regard to internet intermediaries, addressing not only the intermediaries' responsibilities, but also the duties and obligations of States with regard to internet intermediaries' services.

4. As stated in the draft recommendation internet intermediaries fulfil a crucial role in providing significant public service value. Although the scope and nature of their activities vary, these services (and their providers) are becoming increasingly central to the constitution of a democratic public arena, with several implications for public debate, self-determination concerns and the enjoyment of human rights in general.

5. The Bureau of the Committee of Convention 108 fully subscribes to the declaration, in the Preamble, stating that "In line with the jurisprudence of the European Court of Human Rights, the Council of Europe member states have the obligation to secure to everyone within their jurisdiction the rights and freedoms contained in the Convention for the Protection of Human Rights and Fundamental Freedoms both offline and online". In this sense, the guidelines should explicit that the right to privacy is an enabler to the exercise of other human rights in both environments, increasingly affirming its crucial role in dealing with the challenges and potentials for the protection of human rights brought about by internet. Privacy is a premise for the full exercise of fundamental freedoms, a conception that is reflected in the European Convention on Human Rights: Article 8 precedes the guarantees of freedom of thought, conscience and religion; freedom of expression and freedom of assembly and association. Underpinned by this conception, the Bureau recommends that the Preamble explicitly mentions privacy as an enabling right, including a complement such as the following: *"The right to privacy and data protection is a premise for the on-line enjoyment and exercise of most of the rights and freedoms guaranteed by the ECHR"*.

6. When outlining the challenges related to the task of regulating the services provided by intermediaries in paragraph 4 of the Preamble, one of the elements raised as part of this complexity is "the anonymity of users". Although anonymisation technologies are available and currently in use, the anonymity of users is not the common pattern on internet. Considering that usual internet browsing leaves several digital "footprints" as well as the fact that identification is often possible based on IP addresses and other means, the Bureau of the Committee of Convention 108 considers that the term "anonymity" might not be the most appropriate one to reflect the context outlined in paragraph 4.

7. Regarding the Council of Europe regulatory framework that should be taken into account by member states when implementing the guidelines, mentioned in paragraph 9 of the Preamble, the Bureau of the Committee of Convention 108 recommends adding references to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108); the Recommendation CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling; and the Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data adopted by the Committee of Convention 108.

8. In relation to the duties and obligations of states, the section on “legality” should highlight the application of the principles of necessity and proportionality to the requests, demands and actions by public authorities mentioned in paragraph 1.1.1. As a consequence, measures that interfere with human rights and fundamental freedoms must not only be prescribed by law, but must also constitute a necessary and proportionate measure in a democratic society as provided by Article 8.2 of the ECHR. This should be inserted in the text.

9. The Bureau of the Committee of Convention 108 fully supports the guidelines presented in point 1.2 referring to legal certainty and predictability for which it suggests two punctual modifications. Considering that law enforcement is part of the executive branch, paragraph 1.2.2 should be adapted in order not to imply otherwise. Also, taking into account the most adequate terminology under the applicable international standards, the reference to “personally identifiable information” in paragraph 1.2.3 should be replaced by “personal data”.

10. In line with paragraph 1.2.3, the Bureau of the Committee of Convention 108 underlines that transparency is of paramount importance for truly legal certainty and predictability. In addition to the prescription that “states should make publicly available (…) comprehensive information on the number, nature and legal basis of restrictions of human rights, such as regarding content removal and personal data”, the Bureau recommends the insertion of a clear reference to transparency in relation with transfer of personal data across border, particularly those based on MLAT (Mutual Legal Assistance Treaty) agreements.

11. With regard to the section on “safeguards for privacy and data protection” in point 1.4, the Bureau of the Committee of Convention 108 invites to a clarification of the term “store” in paragraph 1.4.1, i.e. referring to *data retention* or *data preservation* (as defined in Article 16 of the Budapest Convention). Additionally, it is preferable to use the term “personal data of their users” after the reference to *access* and *storage* than refer to “personal information or other data (…)”. In relation to the substantive safeguards for data protection provided in paragraph 1.4.1, the Bureau emphasises that Article 9 of Convention 108 is also a key reference with regard to the limitation of rights and that it should be added after the reference to Article 8 of the ECHR. Moreover, with a view to insert the call for compliance with the principles of necessity and proportionality within the context of democracy and rule of law guarantees, the Bureau suggests modifications as follows: “(…) and must be *used when it is* necessary and proportionate *in a democratic society* to the aim pursued”.

12. Regarding paragraph 1.4.2, the Bureau of the Committee of Convention 108 suggests replacing “regulatory” by “legal” frameworks, since the sentence refers to the set of rules provided by law in each member state. Regarding the same paragraph, the compliance with data processing principles and the guarantee of the rights of the data subjects could, instead of being based on the member states territory, rather be based on their jurisdiction. As for the reference to data protection principles, it is advised to substitute “integrity and confidentiality” for “security” (see Article 7 of Convention 108). Lastly, the Bureau underlines that the full compliance with Convention 108, mentioned in the end of the paragraph 1.4.2, also depends on the performance of an independent authority, which should be stressed as a complement to this guideline as follows: *“(…) in full compliance with the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No.108), providing also for the oversight of an independent authority within the meaning of Article 1 of the Additional Protocol concerning supervisory authorities and trans-border data flows*”.

13. The respect and promotion of the right to confidentiality of private communications should be affirmed as a general rule in the guidelines, as the current wording: “facilitated by internet intermediaries through private messaging services” could unduly restrict this right. Furthermore, the Bureau of the Committee of Convention 108 would welcome a clear reference to the fact that the respect and promotion of this right applies to the content of the communication as well as to traffic data.

14. The Bureau of the Committee of Convention 108 fully supports the provisions prescribed in paragraph 1.4.4, that should refer not only to state surveillance measures, but also to law enforcement activities. In this context, it would be welcomed to reinforce that the legal basis authorising both must be clear and publicly available. Accordingly, a reference to the criteria of “necessary measure in a democratic society” (ECHR, Art. 8.2) and to Article 9 of Convention 108 should be added among the set of rules that

surveillance and law enforcement measures must comply with.

15. In relation to point 1.5, particularly to paragraph 1.5.1, it is crucial to emphasise that the guarantee of the right to an effective remedy by member states implies that the access to non-judicial procedures is ensured along with judicial ones.

16. The second part of the guidelines also provides a comprehensive set of guidelines geared towards the respect for human rights and fundamental freedoms, focusing in turn on the responsibilities of internet intermediaries. With regard to transparency and accountability, paragraph 2.2.2 prescribes that "intermediaries should seek to engage in collaboration and negotiations with consumer associations, human rights advocates, and other organisations representing the interests of users before adopting policies". The Bureau of the Committee of Convention 108 fully supports this participative approach and recommends, as a complement to the consultation of civil society actors, to also include a reference to the Data Protection Authorities. This consultation should take place not only before the *adoption* of internet intermediary policies, but also when *modifying* such policies.

17. The transparency requirements should be further detailed in paragraph 2.2.4 (to be renumbered to 2.2.3) and in paragraph 2.4.3 so as to prescribe that internet intermediaries, when using automated data processing techniques in the performance of their functions, clearly and transparently inform *which data* are processed, with *which criteria* and for *which purposes*. With respect to intermediaries' transparency when using automated data processing techniques in the performance of their functions, the Bureau of the Committee of Convention 108 recommends to complement the paragraph 2.2.3 so as to include that, upon request, the data subject is entitled to know of the reasoning underlying data processing where the results of such processing are applied to him or her and to add to the paragraph 2.4.3: "The person subject to a decision having legal effects concerning her or him, or significantly affecting her or him, taken on the sole basis of profiling, should be able to object to the decision".

18. Regarding paragraph 2.2.5, the transparency reports published by internet intermediaries should also encompass information related to requests for data access and preservation by public authorities. This is a procedure already adopted by internet intermediaries that should be supported and fostered by the guidelines.

19. With respect to paragraph 2.4, which deals specifically with data protection concerns, the Bureau of the Committee of Convention 108 considers that the subtitle "Access to user data" does not fully reflect the myriad of issues addressed in this section as access is only one particular processing operation, while this section is aimed at covering in a broad manner all forms of processing of personal data by internet intermediaries. It could for instance be proposed to refer to the "Use of personal data".

20. With regard to paragraphs 2.4.1 and 2.4.2, they appear to intend to set the key data protection principles applicable to internet intermediaries where they process personal data. The Bureau of the Committee of Convention 108 would propose the following alternative wording for those two paragraphs:

"2.4.1 Internet intermediaries should limit the processing of personal data from users to what is [directly] necessary to provide a service clearly defined and explicitly communicated to all users in a proactive manner. The processing, including collection, retention, aggregation or sharing of personal data must be based on the free, specific, informed and unambiguous consent of the user, with respect to a specific purpose, or on another legitimate basis laid down by law, as prescribed by the Convention for the Protection of Individuals with regard to Automated Processing of Personal Data (ETS No. 108).

2.4.2. Intermediaries should minimise the processing of personal data in light of the purposes for which they are processed. 'Privacy by default' and 'privacy by design' principles should be applied at all stages with a view to prevent or minimise the risk of interference with the rights and fundamental freedoms of users. User data should only be aggregated and migrated across multiple devices or services following the free, specific, informed and unambiguous consent of users. Users should be informed about their rights to review, modify, and delete personal data and to object to the processing of their personal data. They further should be informed about their right to withdraw their

consent at any time in which case all processing of personal data based on the consent of the user should be terminated."

21. It could also be made clear that internet intermediaries should avoid the all-or-nothing approach, allowing the user to consent only with the processing of personal data required to provide the service features in which he or she is interested.

22. The Bureau of the Committee of Convention 108 underlines the absence of a paragraph in point 2.4 addressing the issue of sensitive data as defined in Article 6 of Convention 108. Likewise, this subject should also be mentioned in the first part of the guidelines with respect to duties and obligations of states. This is undoubtedly a crucial matter in relation to the responsibilities of internet intermediaries and public authorities with regard to human rights and fundamental freedoms, demanding specific considerations in the Recommendation. These considerations must emphasise that the processing of special categories of data requires a legal basis and appropriate complementary safeguards such as explicit consent.

23. Another important aspect that should be covered in section 2.4 concerns trans-border data flows. Considering the global reach of many, and certainly the most significant, internet intermediaries and taking into account the flow of personal data between the headquarters and the subsidiaries of these companies (as well as the trans-border nature of access to data by public authorities), regardless where the collection occurred, the Bureau of the Committee of Convention 108 suggests to include recommendations on this matter, to underline that such trans-border data flows should respect the applicable legal conditions.

24. The Bureau of the Committee of Convention 108 fully subscribes to the provisions proposed in point 2.5 in relation to access to an effective remedy and emphasises that the complaint mechanisms have to be available online and offline.

25. An emerging issue that also deserves to be mentioned is the geographical scope of de-indexing. The guidelines can fulfil an important role in setting out standards aligned with the protection of human rights to be applied in the implementation of these measures by internet intermediaries. Data protection concerns arise when, all legal and judicial requirements for a legitimate de-indexing are being fulfilled, this measure is selectively enforced in geographical terms, jeopardising the rights and reasons that originally underpinned such de-indexing decision.

26. Finally, the Bureau of the Committee of Convention 108 emphasises the relevance of such a Recommendation as a key reference for the member states regulations and policies related to the roles and responsibilities of internet intermediaries and welcomes once again this work and the corresponding advance in the respect and promotion of human rights on internet, decisively contributing to the task of protecting the ECHR principles both online and offline.

16 October 2017

OPINION ON THE REQUEST FOR ACCESSION BY THE UNITED MEXICAN STATES

Introduction

On 28 August 2017, the Secretary General of the Council of Europe received a letter dated 25 August 2017 informing him that the United Mexican States wished to accede to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter, "Convention 108" or "the Convention") and to its Additional Protocol regarding supervisory authorities and transborder data flows (hereinafter "Additional Protocol").

The Consultative Committee of Convention 108 would point out that, in 2008, it referred to the Committee of Ministers its recommendation for non-member states with data protection legislation in compliance with Convention 108 to be invited to accede to the Convention. The Ministers' Deputies took note of this recommendation and agreed to examine every accession request in the light of it (1031st meeting, 2 July 2008).

Opinion

In accordance with Article 4 of Convention 108, each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in the Convention (Chapter II). Pursuant to Article 3.1 of the Additional Protocol, the Parties shall regard the provisions of Articles 1 and 2 of the Protocol as additional articles to the Convention and all the provisions of the Convention shall apply accordingly.

Having taken note of the Constitution of the United Mexican States (Articles 1, 16§2, 6A Fraction II, III, VIII, 73, 116 and 133) which respectively guarantee the enjoyment of human rights, the rights to private life and to the protection of one's personal data, data subjects' rights (access, correction, erasure, objection), the institution of an autonomous and independent body in charge of ensuring compliance with the right to personal data protection ("the National Institute of Transparency, Access to Information and Protection of Personal data ", hereinafter "INAI"), its composition, the powers of the Congress of the Union of Mexican States to legislate on this issue and the rank of international treaties in the domestic legal order.

Having examined[7] the Federal Law of 2010 on the Protection of Personal Data held by Private Parties (hereinafter "the Federal Law"), the Regulations to the Federal Law on the Protection of personal Data held by Private Parties of 2010 (hereinafter "the Regulations") and the General Law on the Protection of Personal Data held by Obligated Parties of 2017 (hereinafter "the General Law"), the Committee notes the following:

21. Object and purpose (Article 1 of Convention 108)

The purpose of the Federal Law is set out in its Article 1, namely *"protecting personal data held by private parties, in order to regulate its legitimate, controlled and informed processing, to ensure the privacy and the right to informational self-determination of individuals*".

[7] Legal texts provided with the request:

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

On the basis of an English translation of the laws and regulations.
Original versions are available at:
The Federal Law: http://inicio.ifai.org.mx/LFPDPPP/LFPDPPP.pdf
The Regulations: http://inicio.ifai.org.mx/PROTECCIONDEDATOSPERSONALES/RLFPDPP.pdf
The General Law: http://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017

The purpose of the General Law is laid down in its Article 1, stating that this law "*is the regulatory law of articles 6, Base A and 16, second paragraph of the Political Constitution of the United Mexican States, regarding the protection of personal data held by obligated parties*" and "*its purpose is that of establishing the bases, principles and procedures required to uphold the right of any person to the protection of his/her personal data held by obligated parties*".

These statements comply with the purpose set forth in the provisions of Article 1 of Convention 108.

22. Definitions

The Federal Law sets out the definitions of "personal data", "data processing" and "controller" (Articles 2.a, 2.b, 2.d of Convention 108) in Articles 3(V), 3(XVIII) and 3(XIV) respectively. The Federal Law also includes a definition of the notions of "sensitive data" in Article 3(VI), "data processor' in Article 3(IX), "data owner" in Article 3(XVII) and "transfer' in Article 3(XIX). The Regulations adds a number of definitions to the ones proposed under the Federal Law and notably, the notions of "identifiable individual", "transmission" (Article 2 of the Regulations).

The General Law lays down similar definitions and also includes definitions of the notion of "assessment of impact on the protection of personal data" in Article 3(IV), consent in Article 3(VIII), filing system in Article 3(XII).

I. Personal data (Article 2.a of the Convention)

The Federal Law defines "personal data" as "*any information concerning an identified or identifiable individual*" in Article 3(V).

The General Law provides in Article 3(XXI) for a similar definition and adds to it that "*an individual is deemed to be identifiable when his/her identity may be directly or indirectly deduced from any information*"

Both laws define the data subject (referred to as 'data owner in the Federal Law) as "*the individual to whom the personal data relates*".

This definition corresponds to the one given in Article 2.a of Convention 108.

J. Automatic processing (Article 2.c of the Convention)

Article 3(XVIII) of the Federal Law defines "the processing of personal data" as "*retrieval, use, disclosure or storage of personal data by any means. Use covers any action of access, management, exploitation, transfer or disposal of personal data*".

The General Law lays down a more complete definition of data processing in Article 3(XXIV): "*Any operation or set of operations undertaken by manual or automated means applied to personal data, relating to the retrieval, use, recording, organization, preservation, preparation, utilization, communication, dissemination, storage, holding, accessing, managing, exploitation, release, transfer or disposal of personal data*".

Article 2.c of Convention 108 contains supplementary operations in the open-ended list, which also refers to the "carrying out of logical and/or arithmetical operations" on the data processed, to "alteration" and to "erasure". The Committee considers that the definition of the Federal Law may be understood as a narrower one (the General law refers to 'any operation or set of operations relating to' a particular list of actions, also appearing narrower) which would benefit from further complements, in particular with regard to the operations above-mentioned that are not listed in the definition.

K. Controller of the file (Article 2.d of the Convention)

The Federal Law defines in Article 3(XIV) the data controller as the "*individual or private legal entity that decides on the processing of personal data*." The General Law provides a similar definition in Article 3(IX), except that it applies to obligated parties.

It would be helpful to expand this definition so as to include the detail of the operations carried out which help identifying the controller under Article 2.d of Convention 108, i.e. the decision making on the purpose, the categories of personal data and the operations which should be applied to them.

L. Special categories of data (Article 6 of the Convention)

"Sensitive data" are defined in Article 3(VI) of the Federal Law as "*Personal data touching on the most private areas of the data owner's life, or whose misuse might lead to discrimination or involve a serious risk for said data owner. In particular, sensitive data is considered that which may reveal items such as racial or ethnic origin, present and future health status, genetic information, religious, philosophical and moral beliefs, union membership, political views, sexual preference*." The General Law provides for a similar definition in Article 3(XXVIII).

This definition complies with Article 6 of the Convention (while personal data relating to criminal convictions are not expressly mentioned in this Article, the list given is not an exhaustive one as indicated by the term 'in particular'). Furthermore, such data are covered by a specific chapter of the General Law (Articles 80 to 82) prescribing a specific filing system with reinforced security prescriptions.

The Committee finally notes that the notion of "transfer" in the Federal Law (article 3, XIX) and in the General Law (Title V) does not only relate to transborder data flows, as is the case in Article 12 of the Convention and Article 2 of its Additional Protocol, but also to domestic operations.

23. Scope of the data protection regime (Article 3 of the Convention)

Article 1 of the Federal Law protects "personal data held by private parties" whereas Article 1 of the General Law guarantees "the protection of personal data held by obligated parties", i.e. "*any authority, entity, agency or body of the Executive, Legislative and Judiciary Branches, autonomous entities, political parties, trusts and public funds*" as well as "*Unions and any other individual or legal entity receiving and making use of public funds or acting as authority in the federal, state or local spheres*" (see Article 1, Paragraphs 5 and 6 of the General Law). The purposes of the General Law are further described in its Article 2. The data protection regime therefore applies to both the private sector (The Federal Law) and the public sector (The General Law). This scope corresponds to the scope set out in Article 3 of Convention 108.

"*Persons carrying out the collection and storage of personal data exclusively for personal use and without purposes of disclosure or commercial use*" are not subject to The Federal Law (Article 2(II) of the Federal Law) in compliance with Article 3 of the draft modernised[8] Convention 108.

The Federal Law does not specify that it shall apply "to automated or non-automated processing of personal data", and this double criteria is neither mentioned in the definition of processing (unlike for the General law which specifically refers to "*manual or automated means*" in the definition of the processing).

Besides, Article 2 of the Federal Law specifies that "credit reporting companies under the Law Regulating Credit Reporting Companies and other applicable laws", are not regulated under the Federal Law and are subject to a *lex specialis*[9], which does not contain specific data protection provisions, implying that rights of the data subject granted under the Federal Law are not recognised in a credit reporting context, which would need to be reconsidered.

The Committee is of the opinion that the wording of the Federal Law could be reviewed to reflect the importance of covering both automated and non-automated processing in the scope of application.

[8] See proposed text at: http://www.coe.int/en/web/data-protection/convention108/modernisation

[9] Law to regulate credit information corporations, published in the Official Gazette on 15 January 2002, which notably contains provisions on confidentiality, security measures and rights of 'clients': http://www.banxico.org.mx/disposiciones/marco-juridico/legislacion-de-interes/leyes/%7B3D04AC1C-8A4B-2331-040C-01A03FDAD3B6%7D.pdf

The General Law applies to "*any processing of personal data contained in physical or electronic support mediums, regardless of the mode or manner in which they were created, the type of support, processing, storage and organization*" (Article 4). This appears to be compliant with Article 3 of Convention 108.
Both the Federal and the General laws refer to Public Access Sources. The Committee notes that it would be worth specifying that the data protection legislations apply to the personal data contained in these sources.

Concerning journalism, the Committee notes that the Federal Law does not refer to any derogation to the scope of application of data protection requirements.

24. Quality of data (Article 5 of the Convention)

Article 6 of the Federal Law provides that: "*Data controllers must adhere to the principles of legality, consent, notice, quality, purpose, fidelity, proportionality and accountability under the Law*." Article 7 also guarantees that the personal data is obtained and processed fairly and lawfully. Article 11 ensures that the data is relevant, correct and up-to date and not kept for longer than necessary to achieve the purpose pursued (the Committee notes that Article 11 refers to "personal data contained in databases" and recommends to suppress this limitation). The Committee underlines the requirement under Article 5 of Convention 108 that the purposes be "legitimate", which should be made clearer in the Federal Law for any processing (not solely for the processing of sensitive data). Article 13 deals with the necessity to have a limited purpose and guarantees the data are not used in a way incompatible with this purpose. Article 13 also includes the principle of data minimisation. Although the concepts used are not always called the same as in Convention 108 and it would be worth mentioning explicitly the principle of *fair* processing and adding the concept of *specific* purpose, it can be noted that, generally speaking, the guarantees laid down by the Federal Law correspond to those ensured under Article 5 of Convention 108.

The General Law which provides for the same guarantees (see Articles 16, 18, 19, 23, 25) with, in addition, a reference to the principle of "fairness" (Article 16) complies with Article 5 of Convention 108.

The Committee emphasises that with respect to the processing of data that is contained in publicly available sources (Article 10(II) of the Federal Law and Article 3(XXV) of the General Law), steps should be taken to make sure that the very nature of the data does not risk infringing the data subject's rights and fundamental freedoms.

When it comes to the legitimacy of the data processing, Article 8 of the Federal Law provides that "*all processing of personal data will be subject to the consent of the data owner except as otherwise provided by this Law*" and then describes the characteristics of consent and other legal basis for the processing of personal data (Article 10). The Committee welcomes this introduction and notes that the fact that consent should be "free, specific and informed" is laid down in Article 12 of the Regulations to the Federal Law (the proposed modernised Convention 108 also refers to "unambiguous" consent, thereby excluding the possibility of a tacit consent).

Article 20 of the General Law mirrors these requirements regarding consent for situations where it is the legal basis for the processing and envisages other legitimate grounds for the processing.

These provisions comply with Article 5 of Convention 108.

25. Special categories of data (Article 6 of the Convention)

Special categories of data are defined in Article 3 of the Federal Law and Article 3(XXVIII) and 21 paragraph 4 of the General Law as above-mentioned (see definitions).

Article 9 of the Federal Law provides that "*in the case of sensitive personal data, the data controller must obtain express written consent from the data owner for processing, through said data owner's signature, electronic signature, or any authentication mechanism established for such a purpose. Databases containing sensitive personal data may not be created without justification of their creation for purposes that are legitimate, concrete and consistent with the explicit objectives or activities pursued by the regulated party*."

Article 7 of the General Law and Article 56 of the Regulations provide for a prohibition of the processing of sensitive data, except where specific conditions are met.

However, Article 7 of the General Law also states that this prohibition does not apply in the cases set forth in Article 22 of the Law, which lists a series of cases where the data subject's consent is not required for the processing of his/her personal data. In particular, Article 22(VIII) holds that consent is not needed "*where the personal data are contained in public access sources*." It is important to note that public access sources might also contain sensitive data, for which automated processing might give rise to discriminatory practices or other adverse effects for the data subjects. The Committee therefore recommends to extend the prohibition of processing of sensitive data without the consent of the data subject to those data contained in public access sources.

Even if health data is categorised as sensitive data, the specific nature of the processing of health related data is not addressed either in the Federal law or in its Regulations. The General Law does not address these elements either.

The Committee encourages the insertion of specific modalities regarding the processing of health related data.

26. Data security (Article 7 of the Convention)

Article 19 of the Federal Law provides that "*all responsible parties that process personal data must establish and maintain physical and technical administrative security measures designed to protect personal data from damage, loss, alteration, destruction or unauthorized use, access or processing.*
Data controllers will not adopt security measures inferior to those they keep to manage their own information. Moreover, risk involved, potential consequences for the data owners, sensitivity of the data, and technological development will be taken into account." Article 20 of the Federal Law also introduces the concept of notification of security breaches to the data owner (i.e. the data subject).

It is also worth noting the provisions of Chapter III of the Regulations to the Federal Law relating to the security measures for processing personal data which implement a risk-based approach to data security (see in particular Articles 60 and 61).

The General Law mirrors the aforementioned security requirements in its Article 31, includes a risk-based approach to data security in its Article 32 and the notion of documentation of security compliance in its Articles 34, 35, 36. The General Law also provides for an obligation of the data controller to notify a security breach to the data subject and to the INAI (Article 40).

The relevant provisions applicable to the protection of personal data (the Federal law, the Regulations, the General law) comply with Article 7 of Convention 108. It can solely be regretted that the data breach notification to the supervisory authority is not foreseen under the Federal Law or under its Regulations as this would have fully anticipated the modernisation of Convention 108.

27. Additional safeguards for the data subject (Article 8 of the Convention)

Article 15 of the Federal Law provides that "*the data controller will have the obligation of providing data owners with information regarding what information is collected on them and why, through the privacy notice"* and article 16 of the Federal Law details the information which should be contained in the privacy notice. The General Law provides for similar requirements (Articles 26 and 27[10]), which thus correspond to the provisions of Article 8 of Convention 108 and to the principle of transparency of the modernisation proposals.

Under Chapter III of the Federal Law and notably its Articles 22, 23, 24, 25, the rights of the data subject to access, rectification, erasure and objection are guaranteed. The Regulations to the Federal law also include a right of information of the data subject where a decision is made automatically, without human intervention (Article 112 of the Regulations). The General Law provides for similar requirements (Articles 43, 44, 45, 46

[10] It should be noted that the original version of the Law refers to the name of the controller and not to the name of the data subject ("*La denominación del responsable*").

and 47). Article 57 of the General Law also provides for a right to data portability. The Federal Law and the General Law comply with Article 8 of Convention 108.

Furthermore, Article 45 of the Federal Law provides for the right of the "data owner" (i.e. data subject) to submit a claim to the INAI where his/her request to the data controller has not succeeded or is not complied with. This right complies with the requirement laid down in Article 8(d) of Convention 108.

Finally, data subjects may challenge and appeal a decision of the INAI (See Article 56 of the Federal Law and 138 and 144 of the Regulations, , Article 115 of the General law). This complies with Article 1(4) of the Additional Protocol according to which "decisions of the supervisory authorities, which give rise to complaints, may be appealed against through the courts".

28. Exceptions and restrictions (Article 9 of the Convention)

The Federal Law provides for a limitation of the observance of the principles and exercise of the rights established with regard to "the protection of national security, public order, health and safety as well as the rights of third parties" (Article 4 of the Federal Law). The Committee is of the opinion that part of the interests for which the rights under the Federal Law will be restricted could be more narrowly specified and defined ("public order" being a very broad notion for instance).

Moreover, both the Federal Law and the General Law do not restrict the application of certain provisions to processing carried out by the press for the situation where they would result in a limitation of the exercise of freedom of expression.

Chapter II of the General Law, more specifically Article 80, deals with personal data collection and processing by authorities that are competent "*within the purviews of security, law enforcement and the administration of justice*" and limits the application of data protection requirements in so far as is

"*necessary and proportional to allow them to exercise their functions regarding national security, public safety or for the prevention and prosecution of crimes*". A separate Chapter (Petition for review on matters involving national security, Articles 139 to 143) prescribes the review procedure in matters of national security.

Such provisions comply with Article 9 of Convention 108.

29. The supervisory authority (Article 1 of the Additional Protocol)

The Federal Law and the General Law seem to establish two different entities to ensure compliance with their respective requirements.

Article 38 of Chapter VI of the Federal Law provides for the establishment of a Supervisory Authority, entitled "The National Institute of Transparency, Access to Information and Protection of Personal Data (INAI)", responsible for ensuring compliance with the measures in domestic law giving effect to the principles of the Convention, in compliance with Article 1(1) of the Additional Protocol.

Article 39 of the Federal Law details its responsibilities. Article 59 mentions the powers of verifications but, not specifically "of investigation and intervention" as envisaged under Article 1(2)(a) of the Additional Protocol. However, Chapter IX of the Regulations to the Federal Law deals with "inspections" carried out by the INAI. Cooperation with other supervisory authorities is foreseen in Article 39 of the Federal law and Article 89 of the General Law.

Article 89 of the General Law lists a number of attributions of the INAI in addition to those already mentioned, such as the powers to initiate legal proceedings and to refer to judicial authorities in the context of alleged violations of personal data protection by domestic laws (Article 89(VIII)). Paragraphs (XXXII) and (XXXIII) of the same Article also enable the INAI to submit cases of unconstitutionality against "*federal or state laws and any International Treaties signed by the President of the Republic and approved by the Senate, which infringe upon the right to personal data protection*", as well as to promote "*constitutional controversies as contemplated in article 105, section I, clause I) of the Political Constitution of the United Mexican States*." The power to initiate unconstitutionality lawsuits by the INAI is also enshrined in Art. 105, Fraction II, paragraph h of the Constitution.

The composition of the INAI and the modalities of designation of its members are not addressed in the Federal Law or in the Regulations to the Federal Law. They are however addressed in a separate document submitted with the request for accession to Convention 108, entitled “4. Mexico’s supervisory authority”. This document recalls that the INAI has regulatory, information, verification, resolution and sanctioning powers. Besides, it refers to Article 6, Fraction VIII of the Constitution, which was made available to the Committee and which clarifies that the INAI shall carry out its tasks independently, is composed of 7 commissioners, appointed by the House of Senators after an extensive consultation of society, upon proposal of parliamentary groups, with the vote of two thirds of the members present. Commissioners shall be in office for seven years and elect their chief commissioner by secret ballot for a period of three years. Some constitutional requirements guarantee the absence of conflict of interest.

Article 116 of the Constitution also prescribes the establishment at States’ level of autonomous, specialised, impartial and collegiate bodies responsible for data protection.

Activity reported of the INAI is as follows:

General Complaints filed with the INAI (2011-2016)	
Received	1361
Concluded	1294
In Process	72
Verification procedures from July 2011 to Dec. 2016	**179**
Applications received for protection of rights from Jan 2012 to Dec 2016	**728**
Of which substantiated	334
Number of requests received	**883**
Related to access requests	381
Related to Rectification requests	35
Related to Cancellation requests	310
Related to Opposition requests	157
Sanctions	
Sanctions procedures initiated	177
Sanctions procedures concluded	113
Requests regarding the public sector (obligated parties) access and correction	**296 506**
Appeals filed against the response to requests to obligated parties before the INAI	**1101**
Recommendations, models and tools developed by the INAI	
2013	7
2014	6
2015	3
2016	2
2017	3
Training in data protection delivered by the INAI	**116**
Total number of participants to these trainings	10261

Article 10 of the General Law provides for the establishment of “the National System for transparency, Access to Information and Personal Data Protection” (hereinafter “the National System”) to “contribute to maintain the right to personal data protection in full force nationwide, at the three levels of government”. The National System is regulated by the General Law on Transparency and Access to Public Information and other applicable laws and regulations which were not available for this assessment.

The General Law also refers to the INAI (Article 88 of the General Law) and to the General Law on Transparency and Access to Public Information, the Federal Law on Transparency and Access to Public information and other regulations which "may be applicable". These legislations were not made available to the Committee. The General Law also mentions the "Guarantor bodies" (Article 91) without specifying how they differ from other existing and mentioned supervisory bodies and how their respective competences are articulated. It seems that the National Institute is the competent supervisory body at Federal level and the Guarantor bodies are competent at Federate level but this remains unclear. Consequently, the Committee notes that the provisions of the General Law relating to the National System, the INAI and to the Guarantor body should be clarified to clearly explain the allocation of competences between these different competent bodies.
Articles 146 and 147 deal with the oversight and verification powers of the Institute and the Guarantor bodies.

These provisions comply with Article 1 of the Additional Protocol.

30. Sanctions and remedies (Article 10 of the Convention)

The Federal Law provides for administrative sanctions under Article 64 in the event of a violation of the Federal law as listed in Article 63. It provides for criminal sanctions under Chapter XI and, more specifically, Articles 67 to 69. In particular, Article 64 provides for several administrative sanctions which vary from a simple warning to a fine from 100 to 320 000 of the current Mexico City minimum wage. These sanctions may be doubled when the data processing in question contains sensitive data. Articles 67 to 69 provide for criminal sanctions which vary from three months to five years of imprisonment and will be doubled if sensitive data are concerned.

The General Law also provides for administrative sanctions available to the INAI or the Guarantor bodies (Article 152) which range from public warning to monetary sanctions going from one hundred and fifty to one thousand five hundred times the daily value of the Unit of Measure and Updating (Article 153).

Individuals can file a complaint to the Supervisory Authority (Article 45 of the Federal Law) or in court. Private parties can file a petition for annulment against decisions issued by the Institute with the Federal Law and Administrative Court (Article 56). Under the General Law, "*the data subject may file a petition for review or appeal with the Institute or the Guarantor bodies, as appropriate, or else with the Transparency Unit*" (Article 94). Besides, resolutions taken by the Guarantor Body may be appealed before the INAI (Article 117).

These provisions comply with Article 10 of Convention 108.

31. Transborder flows of personal data (Article 12 of the Convention and Article 2 of its Additional Protocol)

Chapter V of the Federal Law concerns international transfers and Article 36 prescribes transfer based on the consent of the data subject, while Article 37 provides that:

"*Domestic or international transfers of data may be carried out without the consent of the data owner in the following cases:*

I. Where the transfer is pursuant to a Law or Treaty to which Mexico is party:
II. Where the transfer is necessary for medical diagnosis or prevention, health care delivery, medical treatment or health services management;
III. Where the transfer is made to holding companies, subsidiaries or affiliates under common control of the data controller, or to a parent company or any company of the same group as the data controller, operating under the same internal processes and policies;
IV. Where the transfer is necessary by virtue of a contract executed or to be executed in the interest of the data owner between the data controller and a third party;
V. Where the transfer is necessary or legally required to safeguard public interest or for the administration of justice;
VI. Where the transfer is necessary for the recognition, exercise or defense of a right in a judicial proceeding, and

VII. Where the transfer is necessary to maintain or fulfill a legal relationship between the data controller and the data owner."

Section III (Article 74) of the Regulations to the Federal Law relating to international transfers mentions that "*international transfers of personal data will be possible when the receiver of the personal data assumes the same obligations as those of the data controller transferring the personal data*". Article 76 furthermore provides for the possibility to obtain an opinion of the INAI regarding an international transfer.

The General Law also provides that "*all transfers of personal data, whether domestic or international, are subject to the data subject's consent*" (Article 65) and specifies that "*the transfer or transmittal of personal data outside the Mexican territory by the data controller can only take place when the third party recipient or data processor undertakes to protect such data in adherence to the principles and duties established in this Law and the applicable provisions on the matter*" (Article 68).

The principle of adequacy[11] or appropriateness of the level of protection is contained in Article 65 of the General Law which refers to the protection of data *"in adherence to the principles and duties established in this Law".*

Both the Federal and the General Law comply with Articles 12 of the Convention and Article 2 of its Additional Protocol.

Additional comments

The committee welcomes the introduction in the Regulations to the Federal law of the principle of accountability (Articles 47 and 48) and of a risk-based approach to the data processing carried out by the data controller (Article 48, V) thus anticipating the modernisation of Convention 108.

The Committee also welcomes the introduction of the notions of certification (Article 83 of the Regulations to the Federal Law) and of the right to data portability in the General Law.

Conclusion

In light of the above, the Consultative Committee considers that the legal framework on data protection of the United Mexican States generally complies with the principles of Convention 108 and its Additional Protocol. The Committee notes that some adjustments to the legal provisions, in line with the comments of the present opinion, would be welcome.

Based on its analysis of the applicable data protection legislation, the Consultative Committee is of the opinion that the request from the United Mexican States to be invited to accede to Convention 108 and to its additional Protocol should be given a favourable response.

[11] The principle of adequacy according to which "the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention [shall take place] only if that State or organisation ensures an adequate level of protection for the intended data transfer" and, "by way of derogation, if domestic law provides for it because of specific interests of the data subjects or legitimate prevailing interests, especially important public interests, or if safeguards which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law" is guaranteed in Article 2 of the Additional Protocol.

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

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[12] 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.

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

[12] 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

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.

33. 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).

M. 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.

N. 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.

O. 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.

P. 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.

34. 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[13].

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

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*[14], 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.

35. 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 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

[14] 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

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.

36. 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.

37. 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.

38. 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[15]), 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.

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".

39. 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).

[15] 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*").

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.

40. 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.

41. 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.

42. 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 :*

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

IX. 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;

X. 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;

XI. 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;

XII. 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;

XIII. 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

XIV. 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[16] 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.

[16] 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.