COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 29 August / août 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.

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.