Nations Unies A/HRC/49/55

Assemblée générale

Distr. générale
13 janvier 2022
Français
Original : espagnol

Conseil des droits de l'homme
Quarante-neuvième session
28 février-1er avril 2022
Point 3 de l'ordre du jour
Promotion et protection de tous les droits de l'homme, civils, politiques, économiques, sociaux et culturels, y compris le droit au développement

La vie privée et la protection des données personnelles dans les pays ibéro-américains : un pas vers la mondialisation ?

Rapport de la Rapporteuse spéciale sur le droit à la vie privée, Ana Brian Nougrères

Résumé

Depuis le début du XXIe siècle, la manière d'aborder les questions relatives à la vie privée et à la protection des données personnelles a évolué de manière très intéressante dans les pays ibéro-américains.

Le présent rapport fait le point de la situation actuelle dans ces pays en ce qui concerne le droit au respect de la vie privée sous l'angle de la protection des données personnelles, en tenant compte du contexte historique et de la dimension internationale. Il examine dans un premier temps l'évolution du système uruguayen au cours des vingt dernières années, qu'il compare à celle des autres pays ibéro-américains, puis analyse la manière dont les systèmes de protection se sont structurés ces dernières années pour donner naissance au système ibéro-américain de protection des données personnelles.

La Rapporteuse spéciale estime que la question examinée dans le présent rapport peut servir d'exemple en montrant comment œuvrer ensemble à l'avènement d'un monde dans lequel les principes relatifs à la vie privée et à la protection des données sont mutuellement reconnus et respectés et donnent lieu à l'application de normes de protection de la vie privée dans l'espace numérique, et dans lequel il est possible de relever les défis de l'intégration et de l'harmonisation, en conservant en permanence une approche éthique respectueuse de la diversité des peuples.

Merci de recycler

I. Introduction

1. La doctrine qui protège la vie privée et les données personnelles résulte des préoccupations croissantes que suscitent les progrès des technologies de l'information et de la communication, qui offrent des possibilités de gestion et de manipulation de l'information de plus en plus nombreuses et susceptibles de porter atteinte à la liberté, à la vie et à la dignité des personnes.

2. L'évolution technologique a conduit à l'émergence d'une nouvelle conception du monde et des formes de communication, de vie sociale, d'éducation et de travail, ainsi qu'à de nouvelles façons d'aborder les problèmes de santé, la culture et le développement social. Dans ce contexte, la doctrine relative au respect de la vie privée et à la protection des données personnelles, qui relèvent des droits humains fondamentaux, n'a jamais été aussi importante pour garantir la dignité humaine en favorisant l'autonomie, la prise de décisions, l'innovation et, en définitive, l'épanouissement même de la personne.

3. L'intelligence artificielle, la technologie de la chaîne de blocs, la rapidité de traitement de l'information, la réalité virtuelle, la réalité augmentée, la biotechnologie, la robotique, l'internet des objets, la vidéosurveillance de masse et l'impression en trois dimensions sont autant de phénomènes qui perturbent et transforment en profondeur la manière dont nous abordons la vie quotidienne.

4. En outre, la pandémie a non seulement accéléré l'expansion du numérique, mais a aussi conduit les personnes à intégrer davantage les technologies dans leur vie, ce qui peut à la fois leur apporter beaucoup et les exposer à des risques importants, notamment sur le plan de la sécurité de l'information, de la vie privée et du traitement des données personnelles.

5. Dans ce contexte, il importe de garder à l'esprit que l'être humain est au centre de tout cadre normatif et que la consécration des droits humains fondamentaux est essentielle à l'épanouissement de la personnalité dans les sociétés démocratiques. La reconnaissance et la protection des droits humains fondamentaux doivent toujours viser à enrichir la vie des personnes, en faisant constamment de l'être humain l'élément central de l'état de droit.

6. Protéger la vie privée et les données personnelles, c'est aussi défendre la dignité, l'égalité et la liberté des personnes, et œuvrer à l'édification d'une société plus égalitaire, dans laquelle le respect de la vie privée n'est pas l'apanage de quelques-uns.

7. Le droit à la vie privée et, en particulier, le droit à la protection des données personnelles permettent de protéger chaque individu, en lui offrant les moyens d'affirmer son autonomie et sa dignité, dans des conditions d'égalité avec les autres. Comme tous les droits, ils doivent être assortis de garanties juridictionnelles effectives. Parce qu'ils garantissent la capacité des personnes de communiquer et d'échanger, ils contribuent de façon déterminante à la fois à l'existence d'une société démocratique et au bon fonctionnement de celle-ci.

8. Les normes en la matière permettent à l'individu de bénéficier de ces garanties dans l'exercice de ses droits fondamentaux en lui offrant les moyens de protéger sa vie privée, sa dignité, l'égalité avec les autres et, en définitive, sa liberté. En particulier, le droit à la protection des données personnelles est essentiel pour favoriser l'épanouissement de la personne dans les sociétés démocratiques et pour garantir l'existence et le fonctionnement d'une société démocratique. Sa réalisation vise à parvenir à une maîtrise des flux de données personnelles, tout en facilitant le commerce.

II. Origines du système ibéro-américain

9. Au début du XXIe siècle, la plupart des pays ibéro-américains possédaient déjà des systèmes de protection des données, qui étaient globalement très différents des systèmes actuels dans la mesure où ils ne reconnaissaient pas expressément le droit à la protection des données personnelles, même si certaines constitutions, comme celle de la Colombie, adoptée en 1991et modifiée en 2003, régissaient déjà les questions de vie privée.

10. Si l'on prend le cas de l'Uruguay, qui est représentatif de la situation générale observée dans les pays ibéro-américains, on constate que le droit fondamental à la protection des données personnelles a toujours été protégé en droit interne, même s'il a considérablement évolué, comme on le verra par la suite.

11. La Constitution uruguayenne − selon une approche que l'on retrouve dans les autres pays ibéro-américains − s'inscrit dans un système de protection de la vie privée et des données personnelles qui, reconnaissant le caractère non exhaustif des droits constitutionnels, admet que l'énumération des droits, des devoirs et des garanties n'en exclut pas d'autres qui sont inhérents à la personne ou propres au mode de gouvernement républicain.

12. De fait, si la Constitution uruguayenne ne consacre pas expressément le droit à la vie privée, son article 7 énonce le droit des habitants de jouir de la vie, de l'honneur, de la liberté, de la sécurité, de leur travail et de leurs biens en étant protégés, et dispose que nul ne peut être privé de ces droits, si ce n'est en vertu de lois établies pour des raisons d'intérêt général.

13. Sur la base de l'article 7 susmentionné, la doctrine uruguayenne distingue une première catégorie de droits fondamentaux (à la liberté, à la vie, à l'honneur, à la sécurité, au travail et à la propriété) qui sont reconnus par la Constitution, préexistent à ce cadre normatif et sont inhérents à tous les habitants du pays en tant qu'individus de l'espèce humaine, d'une seconde catégorie de droits individuels consacrés par la Constitution, qui en substance forment le droit d'être protégé dans la jouissance de chacun des droits préexistants et qui découlent de la réglementation même que le cadre normatif fait de ces droits.

14. Cette approche repose sur trois articles de la Constitution uruguayenne, à savoir l'article 7 déjà mentionné et les articles 72 et 332. Ces articles sont en accord avec une conception jusnaturaliste de la Constitution uruguayenne reconnaissant l'existence de droits qui sont antérieurs mais qui n'ont pas besoin d'être établis par la loi et ne cesseront pas de s'appliquer du fait de l'absence de réglementation expresse. Pour suppléer à une telle réglementation, il sera fait appel aux fondements de lois analogues, aux principes généraux du droit et aux doctrines généralement admises.

15. À cet égard, on citera le droit d'accès, le respect de la vie privée et la protection des données à caractère personnel qui, à l'époque, n'étaient pas expressément reconnus par la loi.

16. Cependant, tous les droits humains nécessitent des garanties effectives, qui ne sont pas automatiquement apportées par la seule inscription des droits dans la loi.

17. À la question de savoir quelles sont les limites de cette prérogative constitutionnelle, on répondra en invoquant le principe de légalité, selon lequel une limite peut être imposée en vertu d'une loi dictée par des considérations d'intérêt général.

18. Si, selon cette approche, la Constitution uruguayenne consacre les droits humains fondamentaux, la simple consécration constitutionnelle n'offre cependant pas les garanties voulues pour protéger les droits fondamentaux à la vie privée, à la protection des données personnelles et à la dignité, tant que ces droits ne sont pas expressément reconnus de manière globale dans l'ordre juridique positif interne. Autrement dit, il existait des limites à l'exercice effectif de ces droits et des garanties visant à leur donner effet.

19. Compte tenu de la nécessité de préciser les dispositions programmatiques de la Constitution qui font référence aux principes généraux du droit et, dans la mesure où ceux-ci englobent les droits humains fondamentaux à la vie privée et à la protection des données personnelles, il convient d'analyser les pactes, les conventions et les déclarations de portée internationale qui leur donnent corps.

20. Si le propos n'est pas ici de faire une étude détaillée des instruments internationaux, on signalera l'importance de principe que revêtent en la matière le Pacte international relatif aux droits civils et politiques, adopté par l'Assemblée générale des Nations Unies dans sa résolution 2200 A (XXI) du 16 décembre 1966[1], la Convention américaine relative aux droits de l'homme (Pacte de San José du Costa Rica)[2], la Déclaration universelle des droits de l'homme, proclamée par l'Assemblée générale des Nations Unies dans sa

[1] Article 17.
[2] Article 11.

résolution 217 A (III) du 10 décembre 1948[3], la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, adoptée par le Conseil de l'Europe en 1981 et modernisée en 2018, les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel, adoptées par l'Organisation de coopération et de développement économiques en 1980 et modifiées en 2013, et la résolution 45/95 de l'Assemblée générale des Nations Unies, en date du 14 décembre 1990, notamment.

21. On citera également, parmi les instruments régionaux importants en Amérique, les Normes de protection des données personnelles pour les États ibéro-américains, approuvées en 2017 par le Réseau ibéro-américain de protection des données.

22. On peut s'interroger sur la place des traités internationaux dans la hiérarchie des normes.

23. En Argentine, l'article 75 (par. 22) de la Constitution confère un rang constitutionnel aux traités internationaux relatifs aux droits de l'homme. Le paragraphe 23 du même article dispose que le Congrès prend des mesures volontaristes pour garantir la pleine jouissance et le plein exercice des droits reconnus dans les traités internationaux.

24. Dans le cas de l'Uruguay, la norme par laquelle un traité est ratifié a rang de loi. Aucune disposition expresse ne définit la place des traités internationaux. Toutefois, il ressort de la doctrine que les droits, les devoirs et les garanties énoncés dans les traités internationaux peuvent être incorporés dans le droit interne et avoir valeur constitutionnelle, du fait qu'ils sont inhérents à la personne ou propres au mode de gouvernement républicain, et peuvent relever par conséquent de la définition de l'article 72 de la Constitution. Il s'agit-là d'une considération essentielle, qui impose d'harmoniser le droit interne avec le droit international en ce qui concerne la vie privée et la protection des données personnelles.

25. De nombreux pays ibéro-américains ont fondé leurs systèmes de protection des données sur des dispositions réglementaires, que l'évolution de la jurisprudence est venue compléter en comblant les lacunes et en formulant des principes essentiels (comme le Costa Rica), tandis que d'autres (comme le Chili[4] et le Pérou[5]) se sont appuyés sur des réglementations sectorielles, complétées par des dispositions-cadres protégeant les données personnelles et le droit d'accès de manière plus ou moins explicite, selon le cas.

26. D'autres cadres réglementaires définissent les données sensibles, comme c'est le cas de l'article 4 de la loi nº 1682/2001 au Paraguay.

27. Certains systèmes régissent l'obligation de consentement exprès, comme c'est le cas en Argentine avec l'article 5 de la loi nº 25.326 et l'article 5 du décret nº 1558/2001, dispositions qui, de 2001 à 2008, ont constitué un cas isolé de réglementation des données personnelles dans les pays ibéro-américains, jusqu'à ce que l'Uruguay renforce son système de protection des données. Les deux pays ont suivi le modèle du système européen de protection.

28. Le recours en *habeas data* est expressément consacré dans certaines constitutions ibéro-américaines, comme c'est le cas au Brésil[6], au Paraguay[7] et en Équateur[8], tandis qu'au Portugal[9] et en Colombie[10], il est reconnu de manière tacite à travers d'autres éléments du

[3] Article 12.

[4] Loi organique constitutionnelle relative aux fondements généraux de l'administration de l'État et décret législatif nº 1/19.653 de 2001, du Ministère-Secrétariat général de la Présidence du Chili.

[5] Loi nº 27489/2001 de juin 2001 régissant les centres privés d'information sur les risques et la protection du propriétaire de l'information.

[6] Article 5 (LXXII) de la Constitution politique de la République fédérative du Brésil de 1988.

[7] Article 135 de la Constitution de la République du Paraguay de 1992.

[8] Article 92 de la Constitution de l'Équateur de 2008.

[9] Article 35 de la Constitution du Portugal de 1976.

[10] Article 15 de la Constitution politique de la Colombie de 1991.

cadre relatif à la protection des données personnelles. Au Brésil[11] et au Mexique[12], le droit d'accès est reconnu.

29. L'apparition du recours en *habeas data* a permis d'améliorer l'efficacité de certains systèmes de garanties et de les moderniser, même si, en général, tous ces systèmes ont été supplantés par le nouveau mécanisme ibéro-américain de protection des données personnelles qui a pris forme ces dernières années.

30. D'une manière générale, les systèmes réglementaires des pays ibéro-américains avaient établi dès la fin du XX^{e} siècle, comme c'était le cas en Uruguay, que même en l'absence d'une disposition régissant expressément les questions de la vie privée et de la protection des données personnelles ou l'*habeas data*, la protection de ces droits humains fondamentaux était assurée par la Constitution, dans la mesure où celle-ci reposait sur une conception jusnaturaliste des droits humains, au même titre que la philosophie qui a inspiré les dispositions analysées plus haut.

31. Toutefois, dans plusieurs pays, le système présentait des limites lorsqu'il s'agissait de préciser les dispositions programmatiques de la Constitution dans l'intention d'appliquer celles qui faisaient référence aux principes généraux du droit d'une manière qui permette de donner effet aux droits à la dignité, à la protection des données personnelles et à la vie privée.

32. Pour compléter cette vue d'ensemble, on citera les dispositions sectorielles que certains pays ont adoptées concernant les données de santé, les données statistiques, les données relatives aux enfants, les dossiers de crédit ou le secret professionnel, notamment.

III. Les étapes de la transformation du système ibéro-américain

33. Trois grandes étapes ont marqué le processus qui a abouti à l'élaboration d'une législation ibéro-américaine sur la protection des données personnelles.

34. La première étape a été la déclaration publiée à l'issue du 13^{e} Sommet ibéro-américain des chefs d'État et de gouvernement qui s'est tenu en novembre 2003 à Santa Cruz de la Sierra (État plurinational de Bolivie), dont le paragraphe 45 est libellé comme suit : « Nous sommes conscients que la protection des données à caractère personnel est un droit humain fondamental et nous réaffirmons l'importance des initiatives réglementaires ibéro-américaines visant à protéger la vie privée des citoyens qui sont énoncées dans la déclaration d'Antigua portant création du Réseau ibéro-américain de protection des données, ouvert à tous les pays de notre Communauté » [traduction non officielle].

35. Dans le même ordre d'idées, les participants à la 27^{e} Conférence internationale des commissaires à la protection des données et de la vie privée, qui s'est tenue en septembre 2005 à Montreux (Suisse), ont réaffirmé, dans la déclaration finale, l'importance que revêtent les activités de ce Réseau au plan international.

36. La deuxième étape a été la Déclaration d'Antigua (Guatemala), adoptée en juin 2003 à la deuxième Réunion ibéro-américaine sur la protection des données personnelles par les représentants de l'Argentine, du Brésil, du Chili, de la Colombie, du Costa Rica, d'El Salvador, de l'Équateur, de l'Espagne, du Guatemala, du Mexique, du Nicaragua, du Paraguay, du Pérou, du Portugal et de l'Uruguay, dans laquelle les délégations :

> « 1. Se félicitent de l'intérêt croissant, de l'attention et de la volonté d'agir exprimés par les pays ibéro-américains en ce qui concerne la protection des données personnelles.
>
> 2. Réaffirment que la protection des données personnelles est un véritable droit fondamental, en particulier pour ce qui a trait au respect de la vie privée et à la faculté de chacun de contrôler ces données et d'en disposer.
>
> [...]

[11] Loi brésilienne n^{o} 9.507 de 1997.

[12] Loi fédérale sur la transparence et l'accès à l'information gouvernementale publique du Mexique du 11 juin 2002.

5. Constatent qu'il est nécessaire d'encourager l'adoption de mesures qui garantissent un degré élevé de protection des données et qu'il convient de mettre en place des cadres réglementaires nationaux qui, sur le fondement de traditions juridiques communes et dans le respect des droits fondamentaux et des intérêts des différents pays, offrent une protection adéquate dans tous les pays ibéro-américains. Ces cadres réglementaires devraient tenir compte des principes essentiels de protection des données reconnus dans les instruments nationaux. À cet égard, les délégations jugent très positives les initiatives réglementaires qui ont été engagées dans plusieurs pays ibéro-américains.

6. Soulignent qu'il importe de renforcer les échanges de données d'expérience entre les pays ibéro-américains, en entretenant une communication et une collaboration permanentes dans le domaine de la protection des données.

7. Décident à cet effet et afin de renforcer et d'approfondir leur collaboration, en s'appuyant sur le Forum permanent établi à la première Réunion sur la protection des données personnelles, de créer le Réseau ibéro-américain de protection des données [...], ouvert aux représentants de tous les pays ibéro-américains.

[...]

8. Sont conscientes que le droit à la protection des données personnelles renforce la primauté du droit et contribue à asseoir la démocratie dans les pays ibéro-américains, ainsi que leur prestige et leur crédibilité à l'ère de la mondialisation. Elles feront donc, dans le respect du cadre juridique et institutionnel en place au niveau national et dans les limites de leurs compétences respectives, les efforts nécessaires pour que la question de la protection des données personnelles soit promue au sein de la Conférence ibéro-américaine, avec la conviction que cela favorisera la diffusion et la connaissance d'un droit fondamental particulièrement important » [traduction non officielle].

37. La troisième étape est la Déclaration de Cartagena de Indias (Colombie) de 2004 dont les signataires, tenant compte du rôle informatif du Réseau ibéro-américain de protection des données, qui permet de comprendre le fonctionnement de la protection des données dans chaque pays, ont décidé d'agir de façon plus volontariste pour obtenir de réelles avancées dans l'échange d'informations sur le sujet, la création d'un conseil permanent d'entraide et la coopération aux fins de l'établissement de documents ou de propositions communes. C'est ainsi que les thèmes suivants ont été abordés dans différents documents adoptés à ce moment-là et pendant les années qui ont suivi : la protection des données dans le secteur financier (Cartagena de Indias, 2004), les perspectives européennes et ibéro-américaines en matière de transferts internationaux de données (Cartagena de Indias, 2004), le secteur des télécommunications et de l'Internet face aux attaques contre la vie privée (Cartagena de Indias, 2004), le secteur commercial et l'utilisation de l'information à des fins de marketing (Cartagena de Indias, 2004), les possibilités de création d'autorités de contrôle dans le contexte latino-américain (Mexique, 2005), l'administration en ligne et les télécommunications (Mexique, 2005), l'accès à l'information publique et la protection des données (Mexique, 2005), le renforcement du cadre normatif et l'harmonisation (Santa Cruz de la Sierra, 2006), le réseau en ligne (Santa Cruz de la Sierra, 2006), les instruments d'autorégulation (Santa Cruz de la Sierra, 2006), le traitement des données de santé en lien avec les dossiers médicaux (Santa Cruz de la Sierra, 2006), et les lignes directrices visant à harmoniser la réglementation applicable en matière de protection des données dans la communauté ibéro-américaine (Cartagena de Indias, 2007). Le Réseau ibéro-américain a continué de mener ce type de travaux jusqu'à ce jour. Il est résulté différents documents, consultables sur son site Web, parmi lesquels des recommandations concernant le traitement des données personnelles sur la santé en période de pandémie (2021), des recommandations concernant le traitement des données personnelles au moyen de services en nuage (2021), une déclaration contre la violence en ligne à l'égard des femmes et des filles (2021), des recommandations générales concernant le traitement des données à l'aide de l'intelligence artificielle (2019), des lignes directrices relatives au respect des principes et des droits qui régissent la protection des données personnelles dans les projets d'intelligence artificielle (2019) et des normes de protection des données personnelles pour les États américains (2017).

IV. Évolution du système ibéro-américain

38. Les systèmes juridiques de protection des données personnelles reposent sur un ensemble de principes qui sont axés sur le respect de la vie privée et le traitement adéquat des données personnelles et qui tiennent également compte de l'importance de favoriser les flux économiques. Ils réglementent les droits et les actes des personnes dont les données sont traitées, et régissent les questions relatives au consentement, aux responsabilités, à la protection différenciée, à la sécurité, aux autorités de protection des données et aux sanctions, entre autres.

39. Les systèmes diffèrent selon la manière dont s'articulent ces éléments. Ainsi, certains systèmes sont basés sur l'autorégulation ou sur des normes sectorielles. Certains s'appuient sur des autorités de protection, tandis que d'autres ne disposent pas de telles autorités, qui agissent de manière proactive et préventive. Il existe aussi des modèles de corégulation auxquels participent les entreprises, les secteurs de l'industrie et du commerce, l'État, les usagers et les organismes de contrôle afin de créer un environnement propice à l'analyse et à une prise de décisions optimale.

40. On peut noter que la plupart des pays ibéro-américains consacrent le droit à la vie privée comme un droit fondamental dans leur constitution, comme expliqué plus haut au chapitre II.

41. En ce qui concerne la protection des données personnelles, qui est également un droit fondamental, des progrès importants ont été réalisés au cours des deux dernières décennies, avec la promulgation de lois fondées sur le système européen de protection des données.

42. Cela implique l'existence d'une loi générale sur la protection des données personnelles, à quoi s'ajoute une série de principes à respecter, parmi lesquels le principe du consentement, en tant que fondement de la légitimité du traitement des données, et le principe de finalité, qui fixe les limites du consentement légal, ainsi que les obligations, droits et responsabilités des différentes parties concernées. Il faut aussi que soit en place une autorité de contrôle, qui doit pouvoir exercer ses fonctions en toute autonomie et être en mesure d'agir *ex ante* à des fins préventives et de prononcer des sanctions *ex post* en cas de non-respect. De plus, tout système de protection des données doit comprendre des instruments juridiques permettant de garantir les droits sur le plan administratif et judiciaire, qui sont normalement complétés par des mécanismes de sécurité informatique.

43. À la fin du siècle dernier, en dehors de l'Espagne et du Portugal, qui s'étaient engagés sur cette voie avec l'Union européenne, les pays ibéro-américains n'avaient pas encore adopté de législation consacrant la protection des données personnelles en général, à l'exception du Chili (loi nº 19.628, de 1999) et de l'Argentine (loi nº 25.326, de 2000). La protection des données personnelles dans les autres pays ibéro-américains reposait sur la conception jusnaturaliste des constitutions nationales, et la défense du droit découlait d'une interprétation de ces constitutions conforme aux traités internationaux et à certaines dispositions applicables du droit interne. Certaines dispositions sectorielles adoptées dans les différents pays venaient également compléter le régime existant en la matière.

44. Progressivement, l'idée de suivre le modèle proposé lors du XIIIe Sommet ibéro-américain des chefs d'État et de gouvernement tenu en 2003 à Santa Cruz de la Sierra et dans la Déclaration de La Antigua a été analysée et diffusée par le Réseau ibéro-américain de protection des données et s'est transformée en tendance.

45. Les pays ibéro-américains qui ont adopté une loi intégrale sur les données à caractère personnel sont l'Uruguay, en 2008[13] ; le Mexique, en 2010[14] ; le Pérou[15] et le Costa Rica[16],

[13] Loi nº 18331, août 2008.

[14] Loi fédérale sur la protection des données personnelles détenues par des acteurs privés, Loi fédérale sur la transparence et l'accès à l'information publique, Loi générale sur la protection des données personnelles détenues par les entités désignées, et Loi générale sur la transparence et l'accès à l'information publique.

[15] Loi nº 29733/2011.

[16] Loi nº 8968.

en 2011 ; le Nicaragua[17] et la Colombie[18], en 2012 ; Panama[19], en 2019 ; le Brésil[20], en 2018 ; l'Équateur[21], en 2021.

46. Pour ce qui est de l'autorité de protection des données, la législation brésilienne en fait un organe de l'administration fédérale indirecte relevant de la présidence de la République[22]. En Équateur, l'article 75 de la loi organique relative à la protection des données personnelles porte création de l'Autorité de protection des données personnelles, qui est publique et indépendante et qui est chargée de superviser l'application de la loi. Au Nicaragua, les articles 28 et 29 de la loi nº 787/2012 portent création de la Direction de la protection des données personnelles, qui est rattachée au Ministère des finances et du crédit public et chargée de contrôler, superviser et protéger les données personnelles dans les bases de données publiques et privées. Le Paraguay dispose d'une loi sur la protection des données personnelles relatives au crédit[23] qui accorde des pouvoirs dans ce domaine à deux autorités : la Banque centrale et le Secrétariat pour la défense des consommateurs et des usagers. L'autorité correspondante en Uruguay[24], à savoir l'Unité de réglementation et de contrôle des données personnelles, relève de l'agence chargée de l'administration en ligne, elle-même rattachée à la présidence de la République. L'autorité panaméenne en matière de protection des données est l'Autorité nationale pour la transparence et l'accès à l'information, assistée par le Conseil pour la protection des données personnelles, qui se compose de neuf membres issus de différents secteurs. En Colombie[25], c'est le Bureau de la protection des données personnelles de la Surintendance de l'industrie et du commerce qui est chargé de contrôler le respect des principes, droits, garanties et procédures prévus par la loi dans le cadre du traitement des données à caractère personnel.

47. Dans tous les cas, il s'agit d'autorités de contrôle qui jouissent d'un degré d'autonomie plus ou moins important dans l'organigramme fonctionnel de l'État et qui sont dotées d'une autonomie technique, même si elles ne disposent pas d'un budget propre.

48. L'Argentine se trouve actuellement dans une situation différente de celle des autres pays ibéro-américains. Alors qu'en 2000, l'Autorité de protection des données personnelles relevait du Ministère de la justice, en 2017, un décret de nécessité et d'urgence a modifié le degré d'autonomie de cette autorité en confiant au chef du Cabinet des ministres la responsabilité de garantir l'exercice effectif du droit d'accès à l'information publique et de contrôler l'application de la loi sur la protection des données personnelles. La même année a été créée l'Agence pour l'accès à l'information publique, chargée de contrôler la protection intégrale des données personnelles afin de garantir le droit à l'honneur et au respect de la vie privée[26]. Les tâches relatives à la protection des données relèvent donc depuis 2017 des attributions de l'Agence pour l'accès à l'information publique.

49. En ce qui concerne les transferts internationaux de données, ceux-ci sont en principe interdits par le système européen de protection des données personnelles. Selon le système européen, qui est le plus strict, certains pays peuvent être reconnus comme présentant un niveau de protection adéquat, ce qui implique que la réglementation des pays tiers tout comme son application pratique soient adaptées au système de l'Union européenne et puissent ainsi être déclarées adéquates au regard de l'article 25 (par. 6), de la directive 95/46/CE du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. L'adhésion à ce système international de reconnaissance du traitement adéquat des données à caractère personnel a des implications considérables, car elle permet le libre échange de données entre les pays concernés et, par conséquent, une

[17] Loi nº 787/2012.
[18] Loi nº 1266/2008 et loi statutaire 1581/2012.
[19] Loi nº 81/2019 sur la protection des données personnelles.
[20] Loi nº13709.
[21] Loi organique sur la protection des données personnelles
[22] Article 55 de la loi générale sur la protection des données personnelles, telle que modifiée par la loi nº 13.853/2019.
[23] Loi nº 6534/2020.
[24] Article 31 de la loi nº 18331 d'août 2008.
[25] Article 19 de la loi statutaire 1581/2011.
[26] Décret nº 899/2017

facilitation importante des services de commerce électronique dans des conditions de confiance et de sécurité.

50. Deux pays ibéro-américains ont ce statut juridique : l'Argentine (depuis le 2 juillet 2003) (décision 2003/490/CE) et l'Uruguay (depuis le 12 octobre 2012) (décision d'exécution 2012/484/UE). Les deux décisions du groupe de travail institué en vertu de l'article 29 de la directive 95/46/CE, par lesquelles l'Argentine et l'Uruguay ont été déclarés comme étant des pays tiers adéquats, soulignent que l'évolution de la protection des données et la manière dont les autorités compétentes appliquent les principes relatifs à la protection des données préconisés par le système européen feront l'objet d'un contrôle. Il est intéressant de noter qu'en 2016, tant la décision 2003/490/CE de la Commission que la décision d'exécution 2012/484/UE, entre autres décisions concernant plusieurs pays considérés comme offrant un niveau de protection adéquat des données à caractère personnel au regard de l'article 25 (par. 6) de la directive 95/46/CE du Parlement européen et du Conseil, ont fait l'objet d'une modification, qui a été adoptée par la décision d'exécution (UE) 2016/2296 de la Commission en date du 16 décembre 2016, au motif que le niveau de protection assuré par les pays tiers était susceptible de changer et qu'il appartenait à la Commission de vérifier régulièrement si la conclusion sur le caractère adéquat du niveau de protection par le pays tiers en question restait objectivement et juridiquement justifiée.

51. Il convient de signaler que l'Argentine a été, en 2000, le premier pays d'Amérique du Sud à adopter une loi conforme au modèle européen de protection des données personnelles. La loi n° 25.326 couvre la protection des données personnelles enregistrées dans des fichiers, registres et banques de données ou par d'autres moyens techniques de traitement des données, qu'ils soient publics ou privés et concernent des personnes physiques ou morales.

52. La loi prévoit un recours en *habeas data* au niveau constitutionnel en ce qui concerne les données à caractère personnel, afin que la personne concernée ait accès à ses données et puisse demander la rectification ou la suppression des données qui sont inexactes ou utilisées à des fins discriminatoires.

53. Les principes généraux relatifs à la protection des données énoncés dans cette loi sont les suivants : légalité, finalité, qualité des données, consentement, proportionnalité, information, catégorie de données, reconnaissance des données sensibles et principe de sécurité des données.

54. Le système argentin consacre également les droits d'accès, de rectification et d'annulation, ainsi que le droit à l'information dans le cas des bases de données publiques.

55. L'Uruguay a été le deuxième pays à suivre ce modèle, avec l'adoption en août 2008 d'une loi générale (loi n° 18331) qui s'applique aux données enregistrées sur tout type de support, dans le domaine public comme dans le domaine privé, concernant des personnes physiques ou morales, avec quelques exceptions.

56. Les principes sur lesquels repose le système uruguayen de protection des données sont les suivants : le principe du consentement comme fondement de la légitimité du traitement des données ; le principe de la limitation en raison de la finalité ; les principes de légalité, de qualité et de proportionnalité ; le principe de transparence et le principe de sécurité. Les principes de bonne foi, de responsabilité et de minimisation sont également conformes aux exigences légales.

57. Le système uruguayen de protection des données consacre également les droits d'accès, de rectification, de mise à jour, d'ajout ou de suppression qui reviennent aux personnes dont les données sont traitées, à condition que les critères énoncés par la loi soient respectés, conformément au système européen de protection des données.

58. L'enregistrement des bases de données est obligatoire. De ce point de vue, la loi uruguayenne s'inspire de dispositions normatives qui sont devenues obsolètes. En effet, les dispositions réglementant l'enregistrement obligatoire ont cédé la place à des systèmes de responsabilité volontaires.

59. La loi régit à la fois les procédures administratives et les procédures judiciaires accélérées qui peuvent être engagées par les personnes dont les données sont traitées.

60. Cette approche des questions relatives à protection des données personnelles a eu des répercussions dans les pays ibéro-américains, dont plusieurs ont à leur tour adopté des lois proches du système européen. Ce fut le cas entre 2010 et 2013 de la Colombie, du Costa Rica, du Mexique, du Nicaragua et du Pérou. Déjà à l'époque, l'établissement d'un système ibéro-américain de protection des données était considéré comme un objectif à poursuivre.

61. Les pays ibéro-américains avaient ainsi entrepris non seulement de façonner un système commun de protection des données personnelles, mais aussi d'édifier un modèle d'harmonisation et de coopération qui était tourné vers l'Union européenne et visait à faciliter les échanges économiques, tout en protégeant le droit fondamental au respect de la vie privée et à la protection des données à caractère personnel.

V. État actuel du système ibéro-américain

62. Le Règlement général sur la protection des données (règlement (UE) 2016/679) de l'Union européenne, adopté en 2016 et entré en vigueur en 2018, a eu un impact majeur dans le monde entier, y compris dans l'espace ibéro-américain.

63. Parmi les modifications imposées par le Règlement figurent notamment l'établissement d'un système de protection des données mettant l'accent sur les mécanismes de responsabilité volontaire et supprimant le caractère obligatoire de l'enregistrement, la mise en place de dispositifs de protection de la vie privée dès la conception ou par défaut, la réglementation des études d'impact, la réglementation du droit à la portabilité des données, l'obligation de signaler les failles dans les systèmes de sécurité et l'adoption de sanctions plus sévères pour les cas de non-respect.

64. Bien que les pays ibéro-américains aient rapproché leur système juridique du Règlement général sur la protection des données de l'Union européenne, aucune législation n'a pleinement intégré les normes européennes et peu de pays latino-américains ont adopté des dispositions reprenant les innovations du Règlement.

65. Toutefois, les lois sur la protection des données adoptées après l'entrée en vigueur du Règlement (2018) en suivent les grandes lignes et reposent sur une approche conforme au système actuel de l'Union européenne. C'est le cas au Brésil (2018), au Panama (2019), en Andorre (2021) et en Équateur (2021). D'autres pays ibéro-américains alignent progressivement leurs systèmes juridiques sur les dispositions du Règlement.

66. L'Équateur a approuvé le 26 mai 2021 la loi organique sur la protection des données personnelles (loi n° 459), qui suit les principes du Règlement général sur la protection des données de l'Union européenne, notamment en ce qui concerne les garanties exigées, les droits d'accès, de rectification, d'annulation et d'opposition, le droit à la portabilité et le principe de responsabilité.

67. Le Panama a pour sa part adopté le 26 mars 2019 la loi n° 81, qui est entrée en vigueur en mars 2021. Le décret d'application date de mai 2021. Entre autres innovations, cette loi prévoit le principe de la portabilité des données.

68. D'autres pays, comme l'Uruguay, ont harmonisé les dispositions de leur législation avec celles du Règlement général sur la protection des données de l'Union européenne en prévoyant la fonction de délégué à la protection des données, qui dans certains cas est obligatoire et dont le rôle est de fournir des conseils aux fins de l'élaboration des mesures de protection des données, de contrôler le respect de ces mesures et d'en proposer de nouvelles, et de faire le lien avec l'autorité de contrôle. Certains ont aussi institué l'obligation de procéder à des analyses de l'impact du traitement des données personnelles lorsque les conditions légales à cet effet sont réunies. Le principe de sécurité a été actualisé par la loi n° 19.670 et le décret n° 64/2020, qui respectent également les dispositions du règlement consacrant les principes de responsabilité et de protection de la vie privée dès la conception ou par défaut.

69. Dans le même ordre d'idées, le Costa Rica examine actuellement le projet de loi n° 22388 portant modification de la loi sur la protection des personnes à l'égard du traitement des données à caractère personnel (loi n° 8968). Le projet de loi prévoit la fonction de délégué

à la protection des données, consacre la nécessité de procéder à des études d'impact sur la vie privée, modifie les dispositions relatives à l'enregistrement des bases de données, réglemente le consentement des mineurs et comprend des dispositions relatives à la vie privée fondées sur des considérations semblables à celles sur lesquelles repose le Règlement général sur la protection des données de l'Union européenne.

70. Les paragraphes ci-après passent en revue différents éléments qui font que certains systèmes de protection des données et de la vie privée sont plus exigeants, comme c'est le cas du système européen, et évaluent leur incorporation dans la législation ibéro-américaine.

71. En Équateur, la fonction de délégué à la protection des données est réglementée par l'article 85 de la loi organique sur la protection des données personnelles, adoptée récemment. Au Brésil, cette fonction est prévue par l'article 23 de la loi générale sur la protection des données. En Uruguay, l'article 40 de la loi nº 19.670 et le décret nº 64/2020 réglementent précisément ladite fonction. Au Mexique, l'article 85 de la loi générale sur la protection des données personnelles détenues par les entités désignées contient des dispositions relatives au responsable de la protection des données personnelles, et en Colombie cette fonction est envisagée à l'article 23 du décret nº 1377/2013.

72. En ce qui concerne les failles de sécurité, l'Équateur prend celles-ci en considération à l'article 79 de sa loi organique sur la protection des données personnelles, le Brésil à l'article 48 de sa loi générale sur la protection des données, l'Uruguay au chapitre II du décret nº 64/2020 et le Mexique aux articles 38 et suivants de sa loi générale sur la protection des données personnelles détenues par les entités désignées. L'Argentine ne dispose d'aucune réglementation à ce sujet, mais elle a approuvé une série de recommandations sur la sécurité de l'information, qui n'ont pas un caractère contraignant[27]. Au Costa Rica, les failles de sécurité font l'objet de l'article 38 du règlement d'application de la loi sur la protection des personnes à l'égard du traitement des données à caractère personnel. En Colombie, elles sont visées à l'article 17 de la loi statutaire 1581/2012 et au Panama à l'article 2 (par. 5) de la loi nº 81 de mars 2019. Au Nicaragua, l'article 11 de la loi nº 787/2012 institue une obligation de signalement à l'armée ou à la police nationale. Les dispositions en vigueur obligent à signaler à l'autorité de protection des données et/ou à la personne dont les données ont été traitées qu'un incident de sécurité s'est produit et, dans certains cas, un délai précis est fixé à cet effet.

73. Quant aux études d'impact en matière de protection des données personnelles, le Brésil prévoit celles-ci dans sa loi générale sur la protection des données[28], et le Mexique les a rendues obligatoires depuis 2017[29] dans certains cas précis. En Uruguay[30], elles ne sont obligatoires que lorsque la loi en dispose ainsi et en Équateur, elles sont inscrites dans la loi organique sur la protection des données personnelles de 2021[31]. En Argentine, en Colombie, au Costa Rica et en République dominicaine, les études d'impact ne sont pas obligatoires.

74. Le droit à la portabilité est un autre des changements induits par le Règlement général sur la protection des données de l'Union européenne. En Équateur, il a été inscrit dans la récente loi organique sur la protection des données personnelles, qui dispose ce qui suit : « Toute personne a le droit d'obtenir du responsable du traitement des données qu'il lui remettre les données qui la concernent dans un format compatible, mis à jour, structuré, courant, interopérable et lisible par machine, qui préserve leurs caractéristiques, ou qu'il transmette ces données à d'autres responsables »[32]. Le Panama a également consacré ce droit[33]. Le Brésil a aussi inscrit le droit à la portabilité dans sa loi générale sur la protection

[27] Résolution nº 47/2018.
[28] Article 10, paragraphe 3.
[29] Article 74 de la loi générale sur la protection des données personnelles détenues par les entités désignées.
[30] Article 6 du décret nº 64/2020.
[31] Article 42.
[32] Article 17.
[33] Article 15 (par. 5) de la loi nº 81/2019.

des données[34], tout comme le Chili.[35] El Salvador[36], le Honduras[37] et l'Uruguay[38] ont adopté des dispositions portant spécifiquement sur la portabilité numérique. Au Paraguay[39], le droit à la portabilité n'est protégé que pour les données relatives au crédit.

75. Le système ibéro-américain a donc fait un nouveau pas en avant, étant donné non seulement que le modèle européen traditionnel a été suivi, mais aussi que l'action normative entreprise a mis l'accent sur l'amélioration des moyens de coopération entre les pays ibéro-américains et l'Union européenne.

VI. Conclusions

76. **Les droits des personnes doivent toujours contribuer à renforcer l'égalité et la dignité, l'autonomie et la liberté de la personne humaine, et favoriser la coexistence sociale et politique, dans la mesure où l'individu est à la fois l'origine et la finalité de toute organisation juridique et politique.**

77. **Même en l'absence d'une disposition régissant expressément les questions relatives à la vie privée, à la protection des données personnelles et aux recours en *habeas data*, il existe une protection de ces droits humains fondamentaux, qui repose sur l'approche jusnaturaliste dont les constitutions ibéro-américaines étaient imprégnées jusqu'à la fin du siècle dernier.**

78. **Trois grandes étapes ont marqué l'évolution du système ibéro-américain de protection des données personnelles. Le premier est la Déclaration du treizième Sommet ibéro-américain des chefs d'État et de gouvernement, adoptée à Santa Cruz de la Sierra en novembre 2003. Le deuxième est la déclaration d'Antigua, de juin 2003. Le troisième est la Déclaration de Cartagena de Indias de 2004.**

79. **Dans la plupart des pays ibéro-américains, la Constitution consacre le droit à la vie privée en tant que droit humain fondamental.**

80. **La protection des données personnelles est également un droit fondamental, même si elle n'est pas expressément inscrite dans les constitutions. Depuis le début du XXI^e^ siècle, la tendance dans les pays ibéro-américains a été de promulguer des lois s'inspirant du système européen de protection des données personnelles, qui venaient compléter les dispositions programmatiques de leurs constitutions respectives.**

81. **Ce type de système est caractérisé par l'existence d'une loi générale qui couvre de manière exhaustive les questions relatives aux données à caractère personnel.**

82. **Ladite loi énonce un certain nombre de principes qui doivent être honorés et respectés, ainsi que les obligations, les droits et les responsabilités des différentes parties concernées. Elle prévoit en outre la création d'une autorité indépendante de contrôle du traitement des données personnelles qui peut mener une action préventive et également agir a posteriori en sanctionnant le non-respect des règles. Il est important qu'il existe aussi des instruments juridiques permettant de faire valoir les différents droits en jeu par des voies administratives et judiciaires.**

83. **Il ressort de l'analyse du cadre normatif ibéro-américain qu'il existe un système de protection des données personnelles qui offre un modèle d'harmonisation et de coopération, tourné vers l'Union européenne et tendant à un juste équilibre entre la protection des droits humains fondamentaux et la libre circulation des biens, des personnes, des services et des capitaux, favorisant ainsi une intégration économique et sociale saine.**

[34] Article 18 (V), tel que modifié par la loi n° 13.853/2019.

[35] Article 9 de la loi n° 19.628 du 18 août 1999, telle que modifiée en 2018.

[36] Article 19 e) du décret législatif n° 142 du 6 novembre 1997 sur les télécommunications et l'énergie, tel que modifié en 2008.

[37] Loi sur la portabilité numérique, du 30 avril 2014.

[38] Article 471 de la loi n° 19889 du 9 juillet 2020.

[39] Article 8 de la loi 6534/2020 sur la protection des données personnelles de crédit.

84. **L'approbation et l'entrée en vigueur du règlement général de l'Union européenne sur la protection des données (règlement (UE) 2016/679) ont eu d'importantes répercussions dans les pays ibéro-américains, qui ont adopté les différentes solutions proposées dans le Règlement sur des questions telles que la nécessité de désigner une personne responsable de la protection des données dans chaque organisme, les modalités de signalement et de traitement des incidents de sécurité, les mesures volontaires de responsabilité, l'évaluation des risques potentiels aux différentes étapes du cycle de vie des données et le droit à la portabilité, entre autres.**

85. **Considérant que la coopération est une composante essentielle du système de protection des données personnelles, les pays de l'espace ibéro-américain se sont attachés à harmoniser leur réglementation avec le modèle européen afin de parvenir à un niveau d'intégration élevé avec l'Europe dans ce domaine.**

86. **S'il ressort de l'analyse effectuée que les dispositions et institutions de protection des données ne sont pas toutes prises en compte dans les différentes législations ibéro-américaines, les exemples donnés montrent toutefois que l'on s'achemine clairement vers une protection intégrale de la vie privée et des données personnelles, avec de nettes influences européennes, dans le cadre de ce qui constitue le système ibéro-américain de protection des données personnelles.**

VII. Perspectives

87. On constate, à la lumière de ce qui précède, la mise en place à l'échelle ibéro-américaine d'un système de protection des données personnelles qui se fonde sur les principes européens en la matière. Cette évolution repose sur un mécanisme intéressant de coopération entre les pays ibéro-américains et l'Europe, qui s'est progressivement étendu à une zone géographique de plus en plus large sur le continent américain au cours des deux dernières décennies.

88. Cette façon de procéder pourrait être prise en exemple pour contribuer au renforcement des principes relatifs au respect de la vie privée et à la protection des données dans le contexte mondial, à condition que l'intégration puisse s'effectuer harmonieusement sur la base du respect mutuel, avec moins de discrimination et plus de justice, dans un monde où les principes démocratiques prévalent et où le développement économique des peuples est favorisé, dans la mesure où seule une approche commune de ces principes peut permettre de maîtriser les effets des évolutions technologiques susceptibles de perturber la vie privée, comme c'est le cas de l'intelligence artificielle, de la réalité virtuelle, de la biotechnologie, de l'Internet des objets et de la vidéosurveillance de masse.

89. Ces objectifs sont réalisables, et l'intégration et l'harmonisation devront guider notre action, qui devra toujours aussi tenir compte de la nécessité d'aider les groupes particulièrement défavorisés, dans le respect des normes éthiques et de la diversité.