EDITORIAL

Data Protection in Latin America: An Overview*

I am pleased to present this special *Latin American* issue of the Global Privacy Law Review (GPLR), which will hopefully provide our readers with a useful framework to understand some of the most significant data protection developments in Latin America.

I would like to sincerely thank and congratulate the Guest Editors; Diego Fernández (*Marval O'Farrell Mairal*) and Prof. Dr Rodrigo Momberg (*Universidad Católica de Valparaíso* and *Alessandri Abogados*), both of whom leading data protection experts in Latin America, for their collective efforts in putting together this excellent special edition.

In his *Guest Editor's Note*, Diego Fernández (*Privacy and Data Protection in Latin America*: *The Future of Privacy*) discusses the significant privacy and data protection changes that Latin America has undergone.[1] Fernández further reviews the unprecedented privacy and data protection challenges arising in the context of the Coronavirus diseases 2019 (COVID-19) pandemic in Latin America. He also draws a parallel between Latin America and the European Union (EU) in terms of the protection of personal data.

Similarly, Rodrigo Momberg (*Privacy Law in Chile: Recent Developments*) discusses the protection of personal data as a constitutional right in Chile.[2] His analysis encapsulates recent significant decisions of the Supreme Court of Chile on privacy issues. Momberg also reviews the proposed administrative changes in relation to cybersecurity and, in particular, the recent public consultations on Administrative Regulations on Cybersecurity in Chile. Finally, Momberg discusses the 'Reform Project', which was put in place to bring Chilean legislation in line with international standards and was intended to make Chile a 'safe harbour'.

It also gives me great pleasure to present the Chairs of the Uruguayan and Mexican data protection authorities, Felipe Rotondo and Blanca Lilia Ibarra Cadena, respectively, who have kindly agreed to provide forewords for this special Latin American issue. I am extremely grateful to them for their efforts on this *Editorial*.

Felipe Rotondo, who holds roles as the Chairman of the Executive Board of the Uruguayan Data Protection Authority The Unit for the Regulation and Control of Personal Data (*Unidad Reguladora y de Control de Datos Personales*) (URCDP) and the Chairman of the Ibero-American Data Protection Network (*Red Iberoamericana de Protección de Datos*) (RIPD), explains in his foreword (*Convergence in Personal Data Protection – A Regulator's View*) how Ibero-American countries are working on modernising their data protection frameworks in line with internationally recognized data protection principles.[3]

In particular, Rotondo explains that the URCDP has been playing an active role on the international data protection scene; currently participating in, among others, the Global Privacy Assembly, the Consultative Committee on Convention 108 from the Council of Europe, and the RIPD.

Uruguay has been a success story in terms of data protection in Latin America. Following an official request from its government on 20 October 2008, Uruguay became the second jurisdiction in Latin America, after Argentina,[4] to be recognized by the European Commission in 2012 as a country that ensures an adequate level of protection for personal data transferred from the EU, within the meaning of the EU's former Data Protection Directive (Article 25(6) of Directive 95/46/

Notes

* Special thanks to Andrew Poulton (Managing Associate, Linklaters, London) for reviewing this editorial note. I would also like to sincerely thank Nick Potter (Linklaters, Madrid) for translating the three forewords of this issue. All errors, of course, remain mine.

1 Diego Fernández, *Privacy and Data Protection in Latin America*: *The Future of Privacy*, in this issue, at 108.

2 Rodrigo Momberg, *Privacy Law in Chile*: *Recent Developments*, in this issue, at 110.

3 Felipe Rotondo, *Convergence in Personal Data Protection – A Regulator's View – Prólogo: La Convergencia en Protección de Datos Personales – Una Visión Desde el Regulador*, in this issue, at 112.

4 Commission Decision 2003/490/EC of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina, http://data.europa.eu/eli/dec/2003/490/oj (accessed 22 Apr. 2021).

EC) and the General Data Protection Regulation (GDPR).[5] This finding of adequacy followed the former Article 29 Working Party's earlier favourable Opinion which was adopted in 2010. This examined Uruguay's domestic law and international commitments with respect to the protection of the private lives, freedoms and individuals' rights.[6]

The 1967 Constitution of Uruguay does not expressly recognize the right to privacy and the protection of personal data.[7] Nevertheless, the charter of fundamental rights is not a 'closed list', as Article 72 of the Constitution provides that the listing of rights, obligations and guarantees made by the Constitution does not exclude others that are 'inherent to the human personality', or indeed those that derive from the republican form of government.[8] Further, Article 1 of Act No. 18,331 on the Protection of Personal Data and the *Habeas Data* Action of 11 August 2008 expressly sets out the following[9]:

> *Derecho Humano.- El derecho a la protección de datos personales es inherente a la persona humana, por lo que está comprendido en el artículo 72 de la Constitución de la República.*
>
> Human Right.- The right to the protection of personal data is inherent to the human being and it is therefore included in Article 72 of the Constitution of the Republic. [English translation provided by the author]

In addition to Act No. 18,331, which enabled the European Commission's adequacy finding, in 2018 Uruguay enacted Act No. 19,670 on Accountability and Budgetary Execution Balance Exercise 2017.[10] This Act contained additional provisions (Articles 37 to 40) which were aimed at aligning the Uruguayan data protection framework with the GDPR.[11] More recently, in 2020, Uruguay adopted Decree No. 64/020 on the Regulation of Articles 37–40 of Law No. 19,670 of 15 October 2018.[12] These recent laws set out new GDPR-like provisions on, amongst other things:

- An extension of the territorial scope of the Uruguayan law to include processing activities carried out by controllers and processors which are not established in Uruguay, but which process data in relation to the offer of goods or services to inhabitants in Uruguay or that imply analysis of their behaviour[13];
- Notification of personal data breaches both to data subjects and to the supervisory authority[14];
- An accountability principle[15];
- Data protection impact assessments[16];
- Privacy by design[17] and default[18]; and
- Data protection officer appointments.[19]

Finally, in Uruguay, the application of the legal data protection standards is guaranteed by administrative and judicial remedies, in particular, by the '*Habeas Data*' Action, which enables a data subject to enforce his rights against data controllers with a court order if necessary. Any interested party is also entitled to seek judicial redress for compensation in the form of damages for losses suffered as a result of the unlawful processing of his personal data. Uruguayan legislation also provides for independent supervision carried out by the supervisory authority, the URCDP, which benefits from powers of investigation, intervention and the power to impose sanctions in line with Article 28 of the former EU Directive 95/46/EC (currently Chapter VI of the GDPR).

Notes

[5] Commission Implementing Decision 2012/484/EU of 21 Aug. 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the Eastern Republic of Uruguay with regard to automated processing of personal data, http://data.europa.eu/eli/dec/2012/484/oj (accessed 22 Apr. 2021).

[6] Article 29 Working Party, *Opinion 6/2010 on the Level of Protection of Personal Data in the Eastern Republic of Uruguay*, 0475/10/EN WP 177 (adopted on 12 Oct. 2010), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp177_en.pdf (accessed 22 Apr. 2021).

[7] *Constitución 1967 con las Modificaciones Plebiscitadas el 26 de nov. de 1989, el 26 de nov. de 1994, el 8 de dic. de 1996 y el 31 de oct. de 2004*, https://legislativo.parlamento.gub.uy/temporales/4942559.HTML (accessed 22 Apr. 2021).

[8] *Ibid.*, Art. 72 of the Uruguayan Constitution states: '*La enumeración de derechos, deberes y garantías hecha por la Constitución, no excluye los otros que son inherentes a la personalidad humana o se derivan de la forma republicana de gobierno*'.

[9] *Ley No. 18.331 de Protección de Datos Personales y Acción de Habeas Data*, https://www.impo.com.uy/bases/leyes/18331-2008 (accessed 22 Apr. 2021).

[10] *Ley No. 19.670 Aprobación de Rendición de Cuentas y Balance de Ejecución Presupuestal – Ejercicio 2017*, https://www.impo.com.uy/bases/leyes/19670-2018 (accessed 22 Apr. 2021).

[11] European Data Protection Board, *Evaluation of the GDPR under Art. 97 – Questions to Data Protection Authorities/European Data Protection Board – Answers from the Spanish Supervisory Authority*, https://edpb.europa.eu/sites/edpb/files/es_sa_gdpr_art_97questionnaire.pdf (accessed 22 Apr. 2021).

[12] *Decreto No. 64/020 Reglamentación de los Arts 37 a 40 de la Ley 19.670 y Art. 12 de la Ley 18.331 Referente a Protección de Datos Personales*, https://www.impo.com.uy/bases/decretos/64-2020 (accessed 22 Apr. 2021).

[13] *Ibid.*, at Art. 1.

[14] *Ibid.*, at Arts 3 and 4.

[15] *Ibid.*, at Art. 5.

[16] *Ibid.*, at Arts 6 and 7.

[17] *Ibid.*, at Art. 8.

[18] *Ibid.*, at Art. 9.

[19] *Ibid.*, at Arts 10 to 15.

In relation to the adequacy decisions, the GDPR states[20]:

> The adoption of an adequacy decision with regard to a territory or a specified sector in a third country should take into account clear and objective criteria, such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country. The third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union, in particular where personal data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States' data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress.

The effect of such an adequacy decision is that personal data can flow from the EU (and Norway, Liechtenstein and Iceland) to that third country without any further safeguard being necessary. Maintaining the free and safe flow of personal data is crucial for businesses and citizens on both sides of the Atlantic.

In the forty-first International Conference of Data Protection and Privacy Commissioners in Tirana between 21–24 October 2019, Rotondo made the following comment while participating in a panel discussing the global convergence in data protection law[21]:

> In this matter it requires an open mind in order to foster data protection effectiveness. Free and safe data flows are needed and that is vital to promote trust in the data protection global system.

In North America, Mexico has followed suit. In other Latin American countries, a similar trend of ensuring protection of personal data has emerged. Blanca Lilia Ibarra Cadena, President Commissioner of the National Institute for Transparency, Access to Information and Personal Data Protection in Mexico (*Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales*) (INAI), describes in her foreword (*Foreword – Prólogo*) how several Latin American countries have taken action to update their existing data protection laws (such as Argentina, Chile, and Uruguay), to approve new laws (such as Panama and Brazil), and to draw up draft legislation (such as Ecuador and El Salvador).[22]

Ibarra explains that, with the introduction of the Federal Law on the Protection of Personal Data Held by Private Parties in 2010, followed by the Governmental Data Protection Law in 2017, Mexico set up a system of rules, principles, duties, and obligations that guarantee data subjects' rights in the private and public sectors, highlighting the role of enforcement agencies in this area.

Article 16 of the Mexican Constitution of 1917 provides extensively for the right to privacy, including protection of the person, family, home, documents or possessions, and the confidentiality of correspondence.[23] The protection of personal data has also been recognized by the Mexican Constitution as a fundamental right since 2009[24]:

> *Artículo 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento. …*
>
> *Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros. …*
>
> Article 16. No person shall be disturbed in his person, family, domicile, papers or possessions, except by virtue of written order from a competent authority, which shall be duly based and justified by the legal cause of the proceedings. ...
>
> Every person has the right to the protection of his personal data, to access, rectify and cancel them, as well as to oppose, as provided by law, which shall set out the exceptions to the principles governing the processing of data, for reasons of national security, public order, public safety and health or to protect third party rights. … [English translation provided by the author]

Following this meaningful recognition, the Federal Law on the Protection of Personal Data Held by Private Parties came into force on 6 July 2010.[25] Subsequently, the Regulations to

Notes

[20] Recital 104 GDPR.

[21] Forty-first International Conference of Data Protection and Privacy Commissioners Conference Report (Tirana 21–24 Oct. 2019), https://globalprivacyassembly.org/wp-content/uploads/2020/08/conference-report.pdf (accessed 22 Apr. 2021).

[22] Blanca Lilia Ibarra Cadena, *Foreword (Prólogo)*, in this issue, at 114.

[23] Teresa Geraldes da Cunha Lopes, *Las recientes reformas en materia de protección de datos personales en México*, 44 Anuario Jurídico y Económico Escurialense 317, 322–323.

[24] *Constitución Política de los Estados Unidos Mexicanos* (5 Feb. 1917), http://www.diputados.gob.mx/LeyesBiblio/pdf_mov/Constitucion_Politica.pdf (accessed 22 Apr. 2021).

[25] *Ley Federal de Protección de Datos Personales en Posesión de los Particulares* (5 July 2010), http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf (accessed 22 Apr. 2021).

the Federal Law on the Protection of Personal Data Held by Private Parties came into force on 22 December 2011.[26] This legislation applies to 'private' individuals or legal entities that process personal data, excluding the Government, credit reporting companies governed by the Law Regulating Credit Reporting Companies or people processing personal data exclusively for personal use.

These laws were supplemented in January 2013 by the Parameters for the Proper Improvement of the Mandatory Self-regulation Schemes referred to in Article 44 of the Federal Law for the Protection of Personal Data in the Possession of Private Parties, which are designed to establish rules, standards and procedures for the improvement and implementation of mandatory self-regulation for the protection of personal data.[27] These Parameters are a combination of self-adopted and mandatory standards, rules and procedures including: (1) procedures to be used for the protection of personal data; (2) procedures to measure the effectiveness of mandatory self-regulation; (3) monitoring and review systems, internal and external; (4) training programmes for those who process personal data; and (5) effective remedies in case of default.[28] The scheme shall establish appropriate sanctions for those who fail in the fulfilment of the mandatory self-regulation such as: warnings, financial penalties, and temporary or permanent suspension of the self-regulation programme.[29]

In January 2017, the General Law for the Protection of Personal Data in Possession of Obligated Subjects was also enacted.[30] 'Obligated Subjects' are defined as any federal, state and municipal authority, public entity, bodies of the executive, legislative and judicial branches, political parties, trusts and public funds.[31]

Later, on 12 June 2018, a decree was published[32] approving the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data dated 28 January 1981 (Convention 108), and its Additional Protocol regarding supervisory authorities and transborder data flows dated 8 November 2001. On 1 October 2018, on the day of the entry into force of the Convention 108 in Mexico, INAI announced that complying with the principles of the Convention 108 would strengthen Mexico's business relations with other signatory countries and establish rules to facilitate data transfers.[33]

In addition to Mexico, Uruguay and Argentina have also ratified the Convention 108 as Latin American non-members of Council of Europe on 10 April 2013 and 25 February 2019, respectively.

Finally, our Editorial Board member Prof. Dr José Luis Piñar Mañas (*Foreword – Prólogo*), who is one of the most influential and pre-eminent figures on privacy and data protection in Spain and Europe, discusses Latin America's journey towards the protection of personal data, through the RIPD.[34] In his words, in Latin America, 'little by little, islets of certainties are forming on a sea of uncertainties about data protection'.[35]

Piñar recites his unique experiences and memories from his various roles as the former Chairman of the Spanish Data Protection Agency (2002–2007), former Vice-Chairman of the Article 29 Working Party (2003–2007), and the first chairman and founder of the RIPD (2003–2007).

I wish to pass on my sincere gratitude to Piñar, to whom I refer to as the 'Godfather' of data protection in Spain, for kindly contributing to the *Foreword* of this issue and, more generally, for supporting the GPLR.

Under the *Articles* section, Luiza Jarovsky (*Dark Patterns, Privacy and the LGPD*) examines the topic of dark patterns in personal data collection (DPPDC).[36] She argues that DPPDC went unnoticed by the lawmakers and privacy advocates, and that data protection laws such as the Brazilian *Lei Geral de Proteção de Dados* (LGPD) do not offer sufficient protection against them.[37]

Jarovsky introduces the general concept of 'dark patterns', followed by a legal analysis of DPPDC, and argues

Notes

[26] *Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares* (21 Dec. 2011), http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf (accessed 22 Apr. 2021).

[27] *Parámetros para el correcto desarrollo de los esquemas de autorregulación vinculante a que se refiere el artículo 44 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, https://dof.gob.mx/nota_detalle.php?codigo=5284967&fecha=17/01/2013 (accessed 22 Apr. 2021).

[28] Linklaters, Data Protected – Mexico (Mar. 2020), https://www.linklaters.com/en/insights/data-protected/data-protected—mexico (accessed 22 Apr. 2021).

[29] *Ibid.*

[30] *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados* (26 Jan. 2017), http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf (accessed 22 Apr. 2021).

[31] *Ibid.*, at Art. 1.

[32] Decreto por el que se aprueba el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y su Protocolo Adicional relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos, hechos en Estrasburgo, Francia, el 28 de enero de 1981, y el 8 de noviembre de 2001, respectivamente, http://www.dof.gob.mx/nota_detalle.php?codigo=5526265&fecha=12/06/2018 (accessed 22 Apr. 2021).

[33] INAI, *El 1 de oct. de 2018 entraron en vigor en México el Convenio 108 del Consejo de Europa y su Protocolo Adicional*, Press Release INAI/281/18 (1 Oct. 2018), http://inicio.inai.org.mx/Comunicados/Comunicado%20INAI-281-18.pdf (accessed 22 Apr. 2021).

[34] José Luis Piñar Mañas, *Foreword {Prólogo}*, in this issue, at 117.

[35] *Ibid.*, at 119.

[36] Luiza Jarovsky, *Dark Patterns, Privacy and the LGPD*, in this issue, at 123.

[37] *Ibid.*

that outdated decision making models enabled under data protection laws make such patterns possible.[38]

In particular, Jarovsky examines the recently enacted LGPD, which, according to her, 'emphasizes data subjects' autonomy without offering additional protection against malicious actors' commonly used techniques'.[39] In order to ensure a fair decision making process and adequate levels of protection of privacy against DPPDC, Jarovsky argues that data protection law needs a paradigm change.[40]

Daniel Álvarez-Valenzuela (*The Constitutional System for the Protection of Privacy in Chilean Law*) reviews the protection of privacy and protection of personal data granted under the Chilean Constitution.[41]

Article 19(4) of the Chilean Constitution expressly protects[42]:

> *El respeto y protección a la vida privada y a la honra de la persona y su familia, y asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley.*
>
> The respect and protection of the private life and the honour of the person and his/her family, and the protection of his/her personal data. The processing and protection of such data shall be in the manner and under the conditions laid down by law. [English translation provided by the author]

Further, Article 19(5) of the Chilean Constitution expressly protects[43]:

> *La inviolabilidad del hogar y de toda forma de comunicación privada. El hogar sólo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinados por la ley.*
>
> The inviolability of the home and any type of private communication. The home may only be searched and private communications and documents intercepted, opened or inspected in the cases and forms determined by the law. [English translation provided by the author]

Álvarez-Valenzuela notes that, despite the obvious differences between these rights set out under the Chilean Constitution, they do intersect or overlap when applying them to specific facts.[44] Álvarez-Valenzuela argues that this wide scope of protection is essential in order to protect our privacy against the threats and risks posed by the use of digital technologies.[45]

Dr María Solange Maqueo (*Mexico (Non-) Adequacy to European Standards on Personal Data Protection in the Context of Employment*) analyses the main standards and regulations put in place by the EU and the Council of Europe with respect to the privacy and personal data protection of employees.[46] Solange argues that there is currently a tendency to strengthen employees' rights in conjunction with employers' interests and that the European approach is more preventive than reactive.[47]

According to Solange, while the Mexican data protection framework is strongly influenced by the European approach, it does not follow this preventive rather than reactive trend.[48] She explains this difference by reference to the asymmetrical rules between the public and private sector, as well as the lack of specific data protection regulation in the context of employment.[49]

Our Editorial Board member Héctor E. Guzmán Rodríguez (*Data Protection in Mexico: One Right, Two Systems, Different Protections and Uncontrolled Data Breaches*) analyses Mexico's 'binary' data protection framework.[50]

As discussed above, there are two main data protection laws in Mexico. One applies to companies and individuals processing personal data for non-household activities, and the other provides a framework for the Mexican States to regulate the data processing activities of the public entities identified as '*Sujetos Obligados*' (Obligated Subjects).

Guzmán argues that, although these laws may seem similar, they set out different rights for data subjects and different obligations for data controllers.[51] He notes that this variance may lead to an inconsistent protection of the data subjects' rights.

Notes

[38] *Ibid.*

[39] *Ibid.*, at 124.

[40] *Ibid.*, at 123.

[41] Daniel Álvarez-Valenzuela, *The Constitutional System for the Protection of Privacy in Chilean Law*, in this issue, at 131.

[42] *Decreto 100 fija el texto refundido, coordinado y sistematizado de la Constitucion Politica de la Republica de Chile*, https://www.bcn.cl/leychile/navegar?idNorma=242302 (accessed 22 Apr. 2021).

[43] *Ibid.*

[44] Álvarez-Valenzuela, *supra* n. 41.

[45] *Ibid.*, at 140.

[46] María Solange Maqueo, *Mexico (Non-)Adequacy to European Standards on Personal Data Protection in the Context of Employment*, in this issue, at 141.

[47] *Ibid.*, at 146.

[48] *Ibid.*, at 147.

[49] *Ibid.*, at 146.

[50] Héctor E. Guzmán, *Data Protection in Mexico: One Right, Two Systems, Different Protections and Uncontrolled Data Breaches*, in this issue, at 149.

[51] *Ibid.*, at 151.

In particular, Guzmán identifies three specific areas where the same individuals (who are data subjects under the legislation) would receive different treatment in relation to the same right, depending on the type of data controller (i.e., a private party and an Obligated Subject): data portability, impact assessments and data breaches notifications.[52]

Sofía Anza & Josemaría Motta (*Data Processors' Liability from a Uruguayan Data Protection Perspective*) analyse the assignment of responsibilities and allocation of liability of the data controllers and processors under the Uruguayan data protection law.[53]

Anza & Motta argue that the processing of personal data has become global and the use of data processors has been increasing over time.[54] The authors note that it is essential to understand how responsibilities are allocated among data controllers and data processors.

Anza & Motta's article provides an overview of the responsibilities and obligations of the data controllers and processors established in Uruguay, or those who are abroad but subject to Uruguayan Data Protection Regulations due to its extraterritorial effect, and explains why this matter should be regulated in further detail.[55]

Finally, under the *Report* section, Guillermo E. Larrea & Juan Carlos Quinzaños (*Privacy in Latin America During COVID-19 Times and Reasonable Digital Security*) provide an overview of the data protection regimes in Latin America and discuss the measures taken in response to the COVID-19 pandemic in the region.[56]

Larrea & Quinzaños examine the factors and circumstances that have affected the region's privacy through this period, including unlawful data processing activities, the design and use of new tracking technologies, remote work, security risks posed by relying too heavily on digital platforms, and specific cybersecurity laws and initiatives in Latin America.[57]

¡Les deseo una buena lectura!
Ceyhun Necati Pehlivan
Editor-in-Chief

Notes

[52] *Ibid.*

[53] Sofía Anza & Josemaría Motta, *Data Processors' Liability from a Uruguayan Data Protection Perspective*, in this issue, at 155.

[54] *Ibid.*, at 156.

[55] *Ibid.*, at 160.

[56] Guillermo E. Larrea & Juan Carlos Quinzaños, *Privacy in Latin America During COVID-19 Times and Reasonable Digital Security*, in this issue, at 162.

[57] *Ibid.*