por los Derechos Civiles

MERCOSUR Electronic Commerce agreement: Challenges and opportunities

July 2022

By Celia Lerman, Gabriela Szlak and Lucía Suyai Mendiberri

Edition: ADC (Association for Civil Rights) and Digital Trade Alliance
Design: Biri Biri
Sponsored by Public Citizen

Executive Summary

On April 29, 2021, at the Mercosur headquarters, representatives of Argentina, Brazil, Paraguay, and Uruguay concluded the Mercosur E-Commerce Agreement (henceforth, the «Agreement»).

In this paper, we will examine its impact on the protection of personal data in the States parties and the development of e-commerce in the region. To do so, we will first evaluate the context in which the Agreement arises, both regarding the exponential growth of domestic e-commerce, especially after the outbreak of the Covid-19 pandemic, and other international agreements, documents, and initiatives within the Mercosur framework. We will then analyze its articles in detail and highlight various examples of its future application.

In addition, we will look at the local regulations of the States Parties, weighing up the impact of the Agreement on central aspects of data protection in each country: international standards, including general principles such as prior consent, purpose, quality, security, accountability, among others; security measures; international data transfers and unsolicited commercial communications. We also compare the Agreement with other international instruments on personal data and the digital economy, including other regional trade agreements such as the Digital Economy Partnership Agreement (DEPA), the Comprehensive and Progressive Trans-Pacific Partnership Agreement (CPTPP), and the Free Trade Agreements between Argentina and Chile, and Uruguay and Chile, with similarities that allow us to conclude that all these texts served as a direct source.

Finally, we offer three main conclusions: 1) Argentina, Paraguay, and Uruguay will have to adjust their local norms on personal data protection to comply with the text of the Agreement; 2) the similarity between the text of the Agreement and other international trade treaties shows the importance for Mercosur to resume international negotiations with the European Union and the CPTPP countries; and 3) the promotion of e-commerce and co-regulation in Mercosur can be positive for the protection of personal data, privacy and human

rights within the region. It is in this fashion that we clarify the opportunities and challenges that the Agreement presents for data protection and the development of digital trade in Mercosur.

Index

1. Introduction

Asociación por los Derechos Civiles (ADC, Association for Civil Rights) is a civil society organization that has been striving for the advancement and defense of fundamental rights in Argentina and Latin America since 1995, with a particular focus on vulnerable persons and social groups. During the last decade, technological innovation has given rise to new risks for the access and exercise of a number of rights, and as a result, ADC has pursued to integrate a digital perspective into its activity.

Since 2020, ADC has been part of the Digital Trade Alliance (DTA), a global coalition that promotes a pro-user/consumer agenda in digital trade discussions. Within the DTA and enjoying the support of Public Citizen, ADC commissioned the renowned lawyers Celia Lerman, Gabriela Szlak, and Lucía Suyai Mendiberri to conduct this research. Following months of intensive activity between late 2021 and early 2022, the authors and ADC's team have jointly arrived at the following considerations.

On April 29, 2021, at the Mercosur headquarters in Montevideo, Uruguay, representatives of Argentina, Brazil, Paraguay, and Uruguay concluded the Mercosur E-Commerce Agreement (henceforth, the "Agreement"). [(1)]

The Agreement is made up of 16 articles, through which it proposes to set up the minimum requirements of a common legal framework for electronic commerce in the jurisdictions of the States parties, in order to take advantage of the economic potential and opportunities that the activity offers. To this end, certain provisions are included for online consumer protection [(2)] in the area of digital trade, and the location of computer facilities [(3)]. It also adopts principles on access to and the use of the Internet for electronic commerce and cooperation between the States [(4)].

In addition, the Agreement establishes the duty of the Member States to ensure the regulation of users' right to personal data protection. In this area, specific

provisions are made on the cross-border transfer of information by electronic means and unsolicited direct marketing.

The main purpose of this paper is to examine the impact of the Agreement on personal data protection in Mercosur countries and the development of electronic commerce throughout the region. To this end, we first review the context in which it arises, considering the exponential growth of this type of business, especially after the outbreak of the Covid-19 pandemic, as well as other international agreements, documents, and initiatives within the Mercosur framework: the Mercosur Digital, the Mutual Recognition Agreement on Digital Signature Certificates, the Mercosur Resolution 37/19 on Consumer Defense and Consumer Protection in Electronic Commerce, and the possible Mercosur - European Union Agreement.

Secondly, we examine the most relevant articles of the Agreement in detail, evaluating their specific text in each case and highlighting various examples of their future application. Thirdly, we look at the local norms of the States Parties, assessing the impact of the Agreement on central aspects of data protection in each country: international standards, including general principles such as prior consent, purpose, quality, security, and accountability, among others.

Fourth, we compare the Agreement with other international instruments on personal data and the digital economy: we review the Council of Europe Convention N°108 and the Standards for Personal Data Protection for Ibero-American States; the Digital Economy Partnership Agreement (DEPA), concluded in 2020 between Singapore, Chile and New Zealand; the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) signed in 2018, and the Free Trade Agreements between Argentina and Chile and Uruguay and Chile, which share similarities with the Mercosur Agreement that allow us to infer that their texts were taken as a direct source.

Finally, we offer three main conclusions: 1) Argentina, Paraguay, and Uruguay will have to adjust their local norms on personal data protection to comply with the text of the Agreement; 2) the similarity between the text of the Agreement

and other international trade treaties shows the importance for Mercosur to resume international negotiations with the European Union and the CPTPP countries; and 3) the promotion of e-commerce and co-regulation in Mercosur can be positive for the protection of personal data, privacy and human rights within the region. It is in this fashion that we clarify the opportunities and challenges that the Agreement presents for data protection and the development of digital trade in Mercosur.

2. Background

2.1. Electronic commerce in Latin America. Effects of the Covid- 19 pandemic[5]

> *"While 2020 will go down in history as one of the most tumultuous years for Latin America's retail industry, it will also be remembered as the year when the region became the world's fastest-growing retail e-commerce market."* [6]

In a world of constant innovation, the growth in the use of Information and Communication Technologies (ICT) in economic matters, and especially in the development of e-commerce, is giving rise to new techniques for marketing products and services. It also brings forth new business models, social and business organization structures, consumption habits, and, last but not least, new regulatory frameworks which, given the lack of significant progress at the multilateral level, are being designed within the domestic and regional spheres. Thus, according to S. Herreros (ECLAC, 2019), preferential trade agreements containing provisions on e-commerce are "very diverse in their breadth and depth, reflecting the different visions of the main players in the digital economy on how such trade should be regulated" [7]. In this sense, the norms at the regional level, and in our particular case, within the Mercosur, are meant to harmonize the different local regulations and thus encourage and promote this new economy in pursuit of taking advantage of the potential and opportunities it entails for the different bloc members.

In the years before the pandemic, both the supply side (companies offering goods and services over the Internet) and the demand side (consumers choosing the Internet as a buying channel) had gradually become more sophisticated in the Mercosur region. The competition to embrace e-commerce shopping within the member countries, particularly in the retail sector, led to constant growth rates and improvements year after year, increasing the quantity and quality of products offered online. As a result, many small and medium-sized enterprises (SMEs) [8] began to offer their products and services by electronic means.[9]

There was also a steady increase in the number of users willing to make online purchases, who, as consumers, were learning and adopting the new technologies available. [10] This trend was grounded on various phenomena such as national and regional policies on digital inclusion, innovation driven by the business sector, the strong penetration of mobile communications with access to Internet services, the growth and professionalization of product and service sales, and the continuous improvement of security and trust in digital transactions, among others [11]. However, according to experts, retail e-commerce in Latin America was still lagging before the pandemic, in its adoption, and even more so, in the cross-border context [12]. In this respect, S. Herreros points out that "in the case of Latin America and the Caribbean, its estimated share in global cross-border e-commerce sales is much lower than its share in global exports of goods, which during the present decade has fluctuated around 5.5%." (2019) [13]

The year 2020 saw a dramatic increase in all e-commerce indicators worldwide, with Latin America as one of its leading regions [14]. According to eMarketers, the effects of the pandemic led the area to become the fastest-growing e-commerce retail industry in the world [15].This record growth is reflected in the 38 million Latin Americans who became first-time digital shoppers in 2020 [16]

It is suggested that the upsurge in electronic shopping could be traced to the effects of the COVID-19 pandemic and the lockdown measures decided by governments to halt its spread. While this unfortunate circumstance proved a disaster to many businesses in terms of physical sales, it became an incredible opportunity for e-commerce which was certainly seized. Thus, throughout the Latin American region, the increase has been much higher than what was expected by pre-pandemic forecasts in all of the countries.

In Brazil, the strongest economy in the bloc, online shopping became the "new normal" in 2021 [17]. The trend was replicated in Argentina, where, according to the Argentinian Chamber of E-Commerce, total digital sales grew by 124% in 2020 [18].

It is believed that the upward trend taken by electronic trade from 2020 onwards is not only here to stay but will continue with no setbacks, even in the face of the return to normalcy in post-pandemic times. The truth is that the growth indicators for online shopping in Latin America in 2020 and the first half of 2021 are, to say the least, impressive.

All the above considered, it can be affirmed that e-commerce has escalated, become bolder, and will continue to open up new opportunities for both supply and demand. Nonetheless, there are a number of problems that still remain within the region. For example, on the demand side, there is a need to increase consumer digital and financial inclusion, while the supply side has the issue of training and professionalization of SME human resources. Besides, there are pending challenges in cross-border e-commerce, both within the bloc and with extra-bloc countries.

At this point, it is worthy to note that in 2020, cross-border electronic trade of tangible goods, already scanty in the region before the pandemic, has tended to decline in both Brazil and Argentina, the two largest economies of the bloc. Consumers in Argentina suffered restrictions in access to cross-border e-commerce, while in Brazil there was a slight growth of 10% in 2019, rising to 14.2% in 2020 [(19)]. Among the circumstances that tend to affect consumers in the region when purchasing foreign goods online, various e-commerce reports have identified: the limitations, increased fees, complexity of tax/customs duties and costs; a perception of insecurity, and lack of trust and diversity in the available means of payment.

From the supply side, there are also some significant barriers for companies wishing to export goods and services through virtual channels. Although an online sales platform or even a social network page can serve as a "showcase" to the world, when trying to arrange a transaction that crosses borders, the supply side, especially SMEs, encounters different sorts of obstacles. For example, in Argentina, although 51% of the companies expressed their interest in selling abroad in 2020, only 7% succeeded in doing so and within that percentage, 58% involved the sale of flights and tour packages, which does not imply

resolving logistics or customs issues of products crossing borders. The reasons identified by the companies as obstacles to international sales were, in order of relevance, logistics, taxes, lack of information, and invoicing issues [(20)].

Hence, we believe that the Agreement is appropriate for both companies and consumers in Mercosur, although there are several issues, beyond the scope of this analysis, that affect the development of cross-border e-commerce. The Agreement aims to initiate a legal framework that harmonizes the norms within the States parties, in order to bolster intra-bloc digital trade and its opportunities for all actors, guaranteeing common rules and addressing, in particular, the rights of consumers and users, among which we find the issues of privacy and personal data protection.

Related to this, we must not overlook the strategic value of data – and not only personal data – as a tradable and intangible asset. In this sense "...cross-border data flows have risen steadily so far this century" [(21)]. Indeed, it has been said that "cross-border electronic commerce, involving agents located in different jurisdictions, is subject to a greater degree of uncertainty than local transactions. In this context, institutional factors are crucial to generate the necessary trust between individuals and businesses. For example, the existence of laws that guarantee an adequate degree of personal data privacy and that protect online consumers against fraudulent practices is essential for people to go ahead and participate in this type of trade.[(22)]"

Finally, the Agreement responds to a trend within Mercosur to unify standards and norms on intra-bloc digital commerce. Resolution 37/2019, regulating Consumer Defense, is an example of this, as well as Consumer Protection in Electronic Commerce, which was recently incorporated into the local laws of each country [(23)], and the Agreement on Mutual Recognition of Digital Signature Certificates [(24)], among others that will be referred to in this document.

2.2. Relevant international agreements, documents, and initiatives in Mercosur

2.2.1. “Mercosur Digital”

In 2017, the Mercosur Digital Agenda Group (“GAD”) was created to “promote the development of a Digital Mercosur”. Some of its main goals are the unification of personal data protection policies, the development of an integrated online mechanism for dispute settlement for e-commerce transactions, and joint projects for the expansion of cross-border digital trade [(25)].

The GAD is responsible for many of the regulations mentioned in this document, such as the Agreement itself, the Mutual Recognition of Digital Signature Certificates, and others.

2.2.2. Agreement on Mutual Recognition of Digital Signature Certificates

The Agreement on Mutual Recognition of Digital Signature Certificates is of great importance to digital trade between the jurisdictions of the party States, since, as its name indicates, its purpose is to recognize the authenticity of the digital signature appearing on each one of its documents [(26)]. Through this accord, digital signatures issued by Trust Service Providers (TSPs) in line with the procedures of each country have the same value as a handwritten signature.

The text establishes certain general guidelines that digital signatures must meet: they should meet international standards, contain data that unequivocally identifies the signatory and the TSP, allow their revocation status to be verified, be issued by a qualified TSP under the national system of accreditation and control of Public Key Infrastructures (PKIs). In addition, the agreement defines a series of operational guidelines for the evaluation and harmonization of certification practices.

At any rate, it should be highlighted that the Digital Signature has not been widely adopted, either among companies selling products and services through e-commerce or among consumers and businesses that buy or sell through the Internet in any of the countries of the bloc. Consequently, we deem that this Agreement does not suffice to guarantee the use of this tool within the bloc, but rather it must be furthered and disseminated by each of the member states.

As to personal data protection, the law merely states that TSPs must conform to the legislation in force in the State where their license or accreditation has been issued.

2.2.3. Mercosur Resolution 37/19. Consumer Defense. Consumer Protection in Electronic Commerce

Mercosur Resolution 37/19 [(27)] creates general criteria to bring in line the norms on Consumer Protection of the States Parties and was duly incorporated into the laws of each country [(28)]. This regulation includes, for example, specific obligations to furnish consumers with information during a business transaction and identify the seller. In addition, it compels suppliers to display the terms and conditions agreement, together with copies of the contract. However, the agreement has no provisions specifically related to personal data protection.

2.2.4. Possible Mercosur - European Union Agreement

In 2019, the text of a possible trade agreement between Mercosur and the European Union was released, including certain provisions on electronic commerce ("Possible Mercosur - European Union Agreement")[(29)] Its targets are to identify possibilities and promote digital trade between the parties and to regulate, were it to be approved, issues such as (i) the principle of technological neutrality of e-commerce;[(30)] (ii) the right to terminate a contract by electronic means [(31)]; (iii) the recognition of electronic signatures' validity; [(32)] (iv) unsolicited marketing communications [(33)]; and (v) consumer protection, among others.

Concerning electronic commerce and personal data protection, the agreement only addresses the prohibition of unsolicited or direct marketing, which basically reflects the principle of consent as a legal ground for handling personal data. However, it then recognizes the right to send this type of communication to consumers with whom there is a relationship and is restricted to products or services similar to those they have previously contracted [(34)]. As will be seen below, a similar text is adopted by Mercosur Agreement, which is the subject of this document.

2.2.5. Free Trade Agreements between Argentina and Chile, and Uruguay and Chile

In 2016, Chile and Uruguay sealed a Free Trade Agreement (FTA) regulating various subjects, including e-commerce.[(35)] The agreement entered into force in 2018. Likewise, Argentina and Chile also concluded a treaty in 2016, moving towards a bilateral integration that came into effect in 2019 [(36)].Regarding provisions on e-commerce (and among them, personal data protection), the text of both documents is very similar, almost replicating that of the Trans-Pacific Partnership (TPP), which later became the CPTPP.

3. The Mercosur Agreement on Electronic Commerce

The purpose of this Agreement, which is the main subject of this paper, is to institute a common legal framework for electronic commerce in the jurisdictions of the States parties in order to take advantage of the economic potential and opportunities that digital trade offers.

The regulation of e-commerce includes personal data protection, as well as other issues that we understand to have implications for it, as will be discussed in detail below.

3.1. Article 1. Definitions

Within the definitions delivered by the Agreement, "personal data" is considered as any information about an identified or identifiable natural person. This characterization is in line with international trends but does not necessarily fit in the current legislation of the bloc member States. For example, in Argentina, Uruguay and Paraguay, the term "personal data" refers to information about legal persons as well.

The article also defines "unsolicited direct marketing communications," which is normally addressed in the personal data laws of each country, As mentioned in previous sections, the protection of personal data in many cases leads to an overall ban on direct marketing communications, with few exceptions, on account of the principle of consent for the use of such information. In this sense, the Agreement describes this type of communication as "an electronic message sent for commercial or advertising purposes to the electronic address of an individual without the recipient's consent, or despite the recipient's explicit refusal." [(37)] This issue is then taken up by the Agreement in article 10, which will be discussed later in this paper.

3.2. Article 2. Scope of application and general provisions

Under its second article, the Agreement states that in considering the potential of electronic commerce as a means of social and economic development, the parties recognize the importance of certain particular issues. It should be stressed that the text is virtually identical to that of Article 11.2 of the Argentina-Chile Free Trade Agreement, which became effective in 2019, as well as Article 8.2 of the Uruguay-Chile Free Trade Agreement, valid since 2018. [(38)]

Regarding the issues considered in this analysis, the following points stand out:
Point 5(b): Encourage self-regulation in the private sector to build up trust and legal certainty in e-commerce, considering the interests and rights of users through initiatives such as guidelines, model contracts, codes of conduct, and trust seals;

Point 5(e): Facilitate the use of electronic commerce by micro, small and medium-sized enterprises and;
Point 5(f): Ensure the security of e-commerce users and their right to personal data protection. A footnote adds that this right refers to the collection and storage of such data, which must be done following general principles on the matter, such as prior consent, purpose, quality, security, and accountability, among others [(39)].

The latter point (f) will be discussed throughout this paper. As to points 2.5(b) and (e), referring to self-regulation for trust and legal certainty in e-commerce, and assistance of SMEs in its use, we understand them as inherently related to particular aspects of personal data protection. The term self-regulation as employed should be seen as a case of co-regulation, as will be developed in section 3.11, under which governments set up a minimum set of norms, while private parties complement the regulatory framework.

3.3. Article 5. Online consumer protection

Under this article, the parties recognize the importance of protecting consumers from fraudulent and deceptive practices when participating in digital trade. In this respect, it states the obligation of Member states to adjust their norms to the MERCOSUR provisions.

It is worth mentioning that the type of consumer protection dictated under this article against fraudulent and deceptive practices is also applicable to the treatment of security and personal data protection within the context of online purchases.

We understand that the States Parties have chosen not to extend on this question due to the disparity between their domestic regulations, as will be seen throughout this paper, since not all of them grant the same levels of protection or have detailed legislation on the subject. Nevertheless, the inclusion of these commitments lays the foundation for the creation of local norms. This is the case of the different resolutions issued by MERCOSUR,

which are then adopted by the countries at the local level. For example, the already mentioned Resolution 37/2019 on Consumer Protection in Electronic Commerce was recently assimilated into the domestic laws of each country. [(40)]

3.4. Article 6. Personal data protection

The Protection of Personal Data is specifically regulated under Article 6 of the Agreement. Interestingly, by way of a statement, paragraph 1 refers to the importance of this protection to build trust in digital transactions. Indeed, this corresponds to the concept of good practice in this field.

Paragraph 2 of the article mandates the Parties to adopt and uphold laws, regulations, or administrative measures to protect individuals' personal information. In this regard, it recommends following the current international standards and norms on the issue.

Paragraph 3 provides that each party should make efforts to ensure that their data protection laws are applied in a non-discriminatory manner. Concerning this, we understand that this type of clause responds to the spirit of regulatory unitization intended by the Agreement, and the trend of trade treaties to adopt provisions such as this one to prevent the norm from becoming a barrier hindering trade.

Also in line with the Agreement's purpose of harmonization, paragraphs 4 and 5 include specific stipulations such as the duty of the States Parties to publish information on the protection recognized to users as of their data, such as the rights of access, rectification, and erasure, as well as to companies of their obligations. Furthermore, clause 8 of Article 6 declares that the parties seek to determine common measures for the protection of personal data and its free circulation within Mercosur. The express commitment of the States Parties to exchange information and experiences regarding their data protection laws is a sign of cooperation towards the development of a common set of norms.

The obligation to implement security measures in the processing of personal data is included in paragraph 6 of this article, expressing that the parties must encourage the use of security, dissociation or anonymization procedures if personal data is handed over to third parties [(41)].

Paragraph 7 affirms that parties must guarantee an adequate level of personal data protection within their jurisdictions through general norms, specific regulations, or mutual agreements. As regards the private sector, it recognizes the possibility of implementing contracts or self-regulatory mechanisms in order to comply with such a level of protection. In this respect, it should be noted that, as mentioned above, the Agreement adheres to a practice of co-regulation, requiring laws and active regulatory action from the government on the one hand, and recognizing the possibility of implementing contracts or self-regulation mechanisms on the other. This provision is also included in Art. 2.5.[(42)]

Self-regulation is the current trend in personal data protection laws, recognizing the capability of private actors themselves to set up a framework that complies with the guidelines dispensed by the norms. This means that self-regulation is acceptable only within the scope laid out by the general regulation and the points specifically stated, all of which configures, in fact, a co-regulation scheme. For example, Argentina determines that adequate levels of protection may come from contractual clauses and self-regulatory systems, adding the provision that such mechanisms must meet the specific resolutions issued by a control authority [(43)].

3.5. Article 7. Cross-border electronic data transfer

Regarding the international transfer of personal data, the Agreement frees the States Parties to determine regulatory standards under the provisions of Article 6.

In turn, paragraph 7, subsection 2 establishes that the transfer must be allowed when it is required for commercial activities, subject to the clauses of Article 6 on adequate levels of protection. Regarding this point, the Agreement

expressly refers to the fact that this may not prevent a State from adopting or maintaining measures to achieve a legitimate public policy objective [(44)]. However, this discretion cannot imply a restriction on trade.

Finally, it is worth mentioning that the terms under the Agreement for cross-border personal data transfer do cover financial services [(45)]. We understand that this exception is to avoid overlapping, as there are already specific regulations on personal data applying to finance. Besides, as we shall see later, the Agreement is inspired by the texts of the CPTPP and the DEPA, which also contemplate specific norms for this activity [(46)].

Countries with existing legislation on international data transfer in financial activities are to interpret this exception restrictively. For example, Argentina and Uruguay expressly consider it only for "banking or stock exchange transfers, concerning the respective transactions and following the applicable legislation."[(47)]

Brazil does not include this exception, for which it would not apply. As to Paraguay, there are currently no regulations regarding transboundary data transfers, but various law proposals have been passed to adjust the norms in the field and do not include an omission of this type. Therefore, the exclusion of financial activities from the general law would not apply either, as in the case of Brazil [(48)].

3.6. Article 8. Location of computer facilities

Article 8 provides that the parties may impose norms relating to computer facilities, including those necessary to ensure the security and confidentiality of communications [(49)].

The same section deals with the principle of territoriality, expressly banning the imposition to locate computer facilities within the territory as a requirement for doing business [(50)]. However, it is foreseen that this may be understood as an obstacle for each government to pursue legitimate public policy

objectives, granting room to accept this type of restriction [51].Thus, despite the express prohibition, States Parties may set up territoriality requirements as long as they are based on the said legitimate reasons. And in order to avoid broad interpretations, the article provides that the aforementioned reasons must not be administered in such a way as to imply arbitrary or unjustifiable discrimination or a disguised restriction on international trade [52]. In this sense, we understand that the Agreement seeks to prevent arbitrary discrimination against technology suppliers, as well as constraints to development, in agreement with the view of some authors [53].

Likewise, by introducing the article on territoriality, it is explicitly stated that housing personal data outside the territory is to be considered a cross-border transfer. Once again, it is clarified that these provisions will not be applicable to financial services.

Finally, it is to be said that there are incipient discussions in some MERCOSUR countries as to the convenience of establishing localization rules. In Argentina, for example, a "Data Sovereignty" bill was introduced in 2017, prescribing that certain data generated by the public sector be stored exclusively in Argentinian territory. Its purpose was to maintain and guarantee access to and safeguard such data under the country's current regulations [54].These discussions might be an explanation for the apparent ambiguity of the Agreement, explicitly banning and then allowing States Parties to territoriality requirements based on legitimate public policy reasons, as well as other specifications seeking to avoid putting up barriers to the development of electronic commerce.

3.7. Article 9. Principles on access to and use of the Internet for electronic commerce

Through this article, States Parties recognize the benefits of people connecting to end-user devices of their preference – subject to the technical regulations of each country – as well as accessing and using online services and applications, thus having information about the network practices of the Internet service provider that may influence their consumer choices. Although the concept

is not conclusively stated in the document, the aforementioned conditions appear to embody a certain principle of net neutrality that is beyond the scope of this paper.

Ultimately, we consider that this declaration reinforces the States Parties' commitment to building the necessary conditions for e-commerce development.

3.8. Article 10. Unsolicited direct marketing communications

EConforming with the applicable regulations on direct marketing practices, Section 10 of the Agreement declares that end-users shall be effectively protected against unwanted commercial communications [(55)]. The text is identical to that adopted in the possible agreement between Mercosur and the European Union in Article 48, which is why we understand that it should be interpreted in light of the European precepts in this area [(56)].

Article 10 formulates that (i) unsolicited commercial communications must not be sent to consumers without prior consent [(57)] and (ii) that they should be indicated as such, identifying the sender and offering the necessary information for the user to exercise their right of withdrawal – also known as the right of opposition –, in other words, to opt out of receiving such messages easily and free of charge.

Regarding consent for unsolicited communications, the article states that it shall be defined per the laws and provisions of each State party and that this type of advertising will be allowed as long as the user's data has been collected in the context of a previous sale of a similar product or service. Here it seems relevant to point out that the norms and the reality diverge deeply in the region, and many companies, especially SMEs who are not from the tech sector, generally fail to comply with the minimum requirements for the effective protection of users against unwanted sales messages.

For example, direct marketing communications are often sent to users stored in databases that have not been purged, making it very unlikely to know if consent to receive such calls or messages has been given. This does not mean that they are non-consensual per se, but simply that adequate procedures for ensuring user consent have not been observed. Typical examples of this are marketing actions carried out by physical retail stores collecting their customers' data through surveys.

Another issue that has been observed is that companies lack uniform processes or technologies, or centralized databases. In addition, their systems do not allow the removal of personal data from certain databases, in several databases simultaneously, or they grant a request of removal or blocking from one but not all at the same time.

The problems mentioned above are only some examples that cause users in the region to perceive that companies send them unsolicited direct marketing communications at ease and fail to comply with their demands to stop receiving them.

Nonetheless, and with due regard to these situations, we are in a stage of expansion and professionalization throughout the region, in which businesses specifically dedicated to providing email marketing services for both SMEs and large firms have begun to observe international trends in the area. These companies work under the criteria of valid consent, which they call opt-in. An example of this can be seen in the event called "eMail Marketing Summit", held in Argentina by AMDIA (Spanish abbreviation of the Argentinian Direct and Interactive Marketing Association) together with email marketing companies, which already in 2019 included a section specifically dedicated to personal data protection among the subjects of its talks [(58)]. Besides, the email marketing business has been proving that campaigns based on sending online correspondence yield better results and higher profits when the people receiving adverts are interested in them. In other words, marketing metrics and best practices are aligned with the current regulations and the requirement for consent.

However, it should be noted that automation and personalization techniques are currently widespread in the digital marketing industry, which entails inherent challenges in terms of personal data protection, both within the region and globally. These techniques enable companies to learn about a user's behavior and consumption habits by tracking their online activities and cross-referencing data, which, in combination with profiling technologies, automates and personalizes the messages or calls they receive. This occurs not only through email, but in all types of advertising on platforms, mobile applications, and websites they browse. Current digital platforms, such as search engines, online maps, content platforms, games, mobile applications, and social media, among others, are generally "free of charge", i.e., do not presuppose money transactions. Indeed, what they offer is a regular exchange of information with their users in which the latter "pay" for the service by handing over their data, often unknowingly. This data is then shared on the platforms or collected through tracking techniques and processed by multiple businesses, through the intensive use of sophisticated technologies such as machine learning and specialized algorithms, all of which can be commercially exploited, not only by the platforms themselves but many other companies, through the purchase and sale of customized advertising in real-time, profiled for each user.

Due to these new trends, it could be said that the regulations being discussed in the region are already "outdated," [(59)] while, from a user perspective, the dialogue on advertising and digital marketing versus privacy and human rights is getting deeper and has just begun [(60)].

The controversy on the subject is linked to the intensive application of the techniques mentioned above which, together with the use of big data, generate online advertising practices in many cases invasive and non-consensual, with deep implications on human rights such as privacy. These practices affect the very heart of online business as we know it today, and are a pending account in terms of privacy and rights at a global level.

In this sense, we value certain initiatives to tackle the issue, both from industry and civil society, seeking to promote innovation and development of the digital

economy on an open and accessible Internet while mitigating the inherent risks it poses to human rights such as privacy. One example of these initiatives is MyData, a community that brings together entrepreneurs, activists, academics, corporations, public agencies, and developers, with the mission of empowering individuals to enjoy informational self-determination regarding their data. Despite recognizing the importance of information exchanges and data flows in today's digital economy, MyData works towards an ethical use of personal data through an alternative vision and the dissemination of technical principles for its treatment based on trust. (61)

It has been repeatedly pointed out that in the face of emerging technologies, it is vital to recognize individuals' rights to informational self-determination and empowerment, as proposed by MyData, together with corporate responsibility and government intervention. Joint work between the private and public sectors will lead to a framework in which government plays a key role in assisting individuals as to their rights, and companies in the management of privacy, balancing regulatory oversight and business innovation. In this context, co-regulation, as referred to in previous sections, takes on special relevance, requiring private actors to implement a specific co-regulatory system in order to apply for an official license to process data (62).

3.9. Article 12. Cooperation

Under this article, the parties express their understanding of the global nature of trade, in particular e-commerce, and consequently, the importance of cooperation. Thus, the document only seems to reflect a certain commitment to lay the groundwork for establishing a set of norms through future negotiations. Among other questions, they commit to:

- Work jointly to facilitate electronic commerce, generate best practices and improve opportunities for micro and small enterprises; (63)
- Share information and experience on laws, regulations, and programs in the area of e-commerce, including those related to personal data protection, among others.
- Enable the exchange of structured and standardized data under norms that allow system interoperability and timely access to data transfers.

3.10. Enforcement of the Agreement and Dispute Settlement

The Agreement does not contemplate a specific dispute settlement procedure. Therefore, in the event of non-compliance by a party, the Mercosur Dispute Settlement System, regulated in the "Olivos Protocol (PO in its Spanish abbreviation)," [(64)] will be applicable. According to this scheme, the parties involved must first attempt to resolve the dispute through direct negotiations (PO art. 4). If these direct negotiations fail to reach any agreement, any of the States Parties may directly initiate the Mercosur ad hoc arbitration proceeding (set out in PO Art. 9 et seq.) or submit it first to the consideration of the Common Market Group (PO Art. 6). The rulings of the ad hoc arbitration courts are binding for the States parties to the dispute and reviewable by the Permanent Review Court (PO Art. 26). It should be highlighted that from the initiation of the dispute settlement system in 1998 until the PO became operative in 2004, i.e., during the validity of the Brasilia Protocol and its Regulations approved by the Mercosur Trade Commission Decision (CCM for its Spanish abbreviation) No. 17/98, ten arbitration awards were issued. On the other hand, the Dispute Settlement scheme also provides for previous and parallel stages such as Consultation and Claims procedures, regulated by CCM Directive No. 17/99, the Annex to the Ouro Preto Protocol, and CCM Decision No. 18/02, respectively. Such mechanisms are managed by the MERCOSUR Trade Commission (CCM) and the Common Market Group (GMC).[(65)]

Without prejudice to the applicability of the Mercosur Dispute Settlement System or the parallel or prior Consultation and Complaint procedures, we understand that, due to the nature of the Agreement, it is unlikely that a State Party would denounce the non-compliance of another through the such course of action. And if that were to happen, the Dispute Settlement System, as well as the Consultation and Complaints System, could be activated to resolve the issues raised.

3.11. Co-regulation under the Agreement

Throughout the text of the Agreement, there are some references to "self-regulation" (as in Article 2. f). Self-regulation has been the subject of well-founded criticism as to its effectiveness vis-à-vis the common good. Likewise, its failure to achieve the intended aims has given rise to modern regulations on personal data protection in Europe and the United States.(66) In this regard, it has been argued that private parties prioritize their own benefit and thus, the resulting self-regulation is lenient and not necessarily protective of individual rights. In addition, the process through which self-regulation principles are founded is generally held to be non-transparent.

Hence, it is not only detrimental to rights-holders, but also potential competitors with no participation in the self-regulation program. For example, self-regulation promoted by large companies may lead to costly processes that raise prices, affect consumers and serve as a means to discourage the entry of other firms and small businesses with fewer resources into the market.(67)

Another criticism is related to the enforcement of the norms in question since private parties and corporate interests lack the incentive to apply penalties in the event of non-compliance (68). In some cases, experience has shown the ineffectiveness referred to above. One example can be seen in the case of the Online Privacy Alliance, an organization created in the mid-1990s that set up guidelines for protecting personal data through self-regulatory mechanisms. The guidelines proposed by this Alliance did not protect individuals against the harmful use of data except through an opt-out mechanism, nor did it ban personal data storage. Moreover, some companies that engaged in massive data handling, such as Amazon.com, did not form part of the alliance. These affairs, among others, led the organization itself to recognize its failure, some years later, and support regulatory initiatives coming from governments (69).

Another case exposing the limitations of self-regulatory systems in terms of enforcement was the case of the Network Advertising Initiative (NAI), ultimately incompetent at ensuring abidance by its guidelines and enforcement. (70)

However, in emerging markets, self-regulatory procedures can still be useful, particularly in building trust with consumers and helping them to distinguish between good and bad-behaving companies. In addition, they have proven to be effective in better adjusting to innovation and technological change, and thus, could serve to improve normative frameworks and fill possible gaps in the implementation of standards, while still being a relatively efficient form of regulation.[71] The Organization for Economic Co-operation and Development (OECD) has concluded that the effectiveness of a self-regulatory process depends mainly on four factors: 1) the boldness of the commitments made by participants; 2) the scope of the self-regulation established within the industry; 3) the extent to which the parties adhere to their commitments, and 4) the consequences of failing to observe them.[72] These points can be reinforced by government regulation, generating a mixed regulatory scheme such as "co-regulation".

Due to the mentioned setbacks of self-regulation, the co-regulatory system has been proposed as a means to overcome them. This is a term coined by a school of thought that endorses an oversight framework in which government and industry participate, sharing responsibility for drafting and applying standards. Dennis D. Hirsch describes it as a hybrid system in which the norms issued by the government are complemented [73]. Under this proposal, the government compels the private sector to prioritize the general well-being and, by presenting collaborative plans between the private and public sectors, increases the opportunities for information exchange and cooperation, which in turn engenders better-quality regulation.

Opponents of these co-regulation strategies are skeptical of such advantages and argue, for example, that the private sector will be reluctant to disclose information so as to obtain more lenient norms. However, it is currently presented as an alternative that can be cost-effective and lead to flexible standards of individual privacy protection [74].

According to De Mooy, an effective co-regulatory system in times of big data technologies and data ecosystems requires public policies and norms that include (i) empowerment of individuals through education and portability

rights; (ii) proven responsibility on the side of companies through self-regulatory mechanisms; and (iii) collective responsibility through the use of legally instituted impact assessments [(75)]. Thus, we see that these three points make up a solid co-regulation scheme, which is presented as an oversight design exceeding the results of self-regulation.

As of the Agreement, it is to be noted that although the text refers to "self-regulation" mechanisms, we believe they should be understood as forms of co-regulation [(76)] since they are not intended to replace the existing laws but to complement them. Thus, their advocation should not be interpreted as excluding government control or as a call to substitute it, but as part of a "co-regulation" system.

Within the region, self-regulation processes gained special relevance to promote incipient legislation – in some cases, non-existent at the time of their establishment – and compliance with standards. Thus, on the supply side (i.e., companies and particularly, SMEs), mechanisms such as Trust Seals could be helpful to enhance access to information and training for the observance of best market practices and the applicable laws. This means that the institutions, whether public or private, that issue trust seals do not intend to be a replacement for the current norms. On the contrary, their purpose is to train the companies and entrepreneurs of the region to show their consumers that they respect them. It is also noteworthy that within the Mercosur area, where SMEs play a fundamental role as a driving force of the economy, the encouragement of self-regulation in the private sector as a complement to government action is useful for fostering conformance to law, trust-building, and legal certainty in e-trade. This comes about after the enormous growth and momentum of e-commerce during the COVID-19 pandemic and the number of companies, especially SMEs and entrepreneurs, who shifted to the online mode to survive in a context of a population under lockdown, often without due regard for the proper practices to be adopted.

Several factors have led companies, commerce chambers, and associations to consider trust seals as a valuable option over the years. Some of the advantages

that they offer are:

- An easy roadmap to operate in multiple locations or facilitate adherence to norms and/or industry technical standards.
- Certainty and transparency to companies based in other jurisdictions with which they interact, regarding compliance with regulations and industry standards.
- Transparency and security to clients in terms of service, complaint resolution, account or content termination, fraud prevention, privacy, personal data de-indexing, etc.
- General confidence in consumers by distinguishing "good" and "bad" companies, in terms of behavior as to their fulfillment of the regulations and standards of the e-commerce industry.

From the consumer's perspective, trust seals usually result in a positive experience. When purchasing online, people normally ask themselves questions concerning the reliability of the transaction: Will the product be sent? Will it arrive on the agreed date? What will happen to the credit card data entered on the platform? Is the website safe? Am I likely to be a victim of fraud? What happens if the item is damaged, faulty, or not the one I ordered? Are the returns and refund processes simple? Who pays the costs associated with the replacement? Is this truly the company it appears to be?

Codes of conduct and trust seals are designed to inform these terms in a clear and standardized manner, using comprehensible and friendly language. The way the information is organized and conveyed often makes the difference in creating user and/or consumer trust. These trust frameworks are offered through chambers of commerce, other associations, or private companies operating as "trusted third party" service providers. Similar schemes can emerge as public-private initiatives, with better prospects of success as a model for cross-border trade, operating at the domestic, regional, transatlantic, or even global level. Companies adhere to them voluntarily, as they include applicable regulations or an integrated version of the norms in various countries, technical standards, ethical rules, and good industry practices.

A business can show abidance by these guidelines through either self-managed processes or physical or automated audits. In some cases, less experienced companies look to these norms as a guide that works like a checklist or a roadmap to go online or access new markets, being able to do so with the security of complying with the applicable regulations in each jurisdiction. The process of certification normally starts by including the corporate or brand name on a website list showing the companies subscribed and the Code of Conduct, sometimes even with access to online complaint mechanisms.[77] The company is then allowed to display a seal or badge – an image or logo, together with a link – on its own sites or applications. This will direct users to the website of the "trusted third party", where they can get information on the guidelines and practices as well as the company. Trust seals or similar certifications will also serve as a means to differentiate the company's image, position itself in the market and build trust in its customer base and/or audience. This way, a business can prove to be legitimate and have undergone a certification process that has verified its fulfillment of the standards proposed by the third party, which will typically include the applicable laws. In some cases, other services associated with the seals could be offered.

An interesting case concerning privacy is the Trust Seals on Personal Data Protection offered by the Mexican Internet Association, created in 2007. Although Mexico is not a member state of Mercosur, its e-commerce has similar characteristics to that of the larger countries of the bloc, for which its experience in this and other areas can serve as a regional example. The mentioned case was a joint initiative between the Mexican public and private sectors seeking to stimulate growth in e-commerce through self-regulation and build confidence in privacy aspects considering the absence of regulations on personal data protection at the time. The Mexican norms were finally promulgated some years later from the experience gained, while the private sector improved its practices, thus creating an example of co-regulation.

Trust Seals in Mexico were launched in 2007, based on the APEC Privacy Framework, and thus, as its website states, "the Internet Association, in direct collaboration with the Ministry of Economy, through the Program for the

Development of the Software Industry (PROSOFT), and in its eagerness to promote best online practices in Mexico, creates and implements the Internet Association Trust Seals project. mx®, a self-regulatory mechanism in privacy matters, focused mainly on the digital market."[(78)]

At a stage in which Mexico lacked specific regulations on the subject, this project evolved favorably including the norms that were finally dictated. At present, the Mexican Internet Association continues to promote Trust Seals, awarding badges to websites belonging to companies, organizations, and physical persons after being evaluated and certifying that they comply with the established requirements and the current regulations. The aim is to build trust. It is worth mentioning that this system coexists with and complements government regulation, for which it could be considered a co-regulation model. Along the same lines, other models of self-regulation and co-regulation have been developed in the region based on trust seals that, for example, provide codes of conduct. For example, we can mention the Trust Seals initiative of the Latin American Institute of Electronic Commerce or currently the eCommerce Institute, which issued a code of conduct including provisions on personal data protection inspired by the regulations in force in Argentina. [(79)] This code has been used to raise awareness among SMEs in the region regarding the applicable norms, in a context in which the Control Authorities were not fully dedicated to actively enforcing them on retail companies, and the population, in turn, was not well-informed and aware of their rights as to personal data protection.

In 2012, the eConfianza initiative, together with the Argentinian Chamber of Electronic Commerce, launched a version of these seals specifically developed for local companies, called "CACE Seals". These were adopted by the chamber's member companies, which were trained in building up consumer confidence through observance of the legal aspects of e-commerce and the active demonstration of such behavior as a strategy to differentiate the firm's image in the market. Businesses that passed the certification process agreed to include their brand in the list of member companies on the CACE Seal website, where each one had a "profile" with information about them available to consumers, among other services.

Both the eConfianza and the CACE seals, targeting companies in the region and Argentina respectively, included a Code of Conduct with a specific section on personal data protection, replicating the current norms and international standards [(80)].

Similarly, we can mention the Code of Ethics of the Direct and Interactive Marketing Association of Argentina (hereinafter "AMDIA", for its abbreviation in Spanish), approved by Provision 4/2004 of the National Directorate for the Protection of Personal Data, with norms especially focused on local companies employing direct marketing strategies [(81)].

These types of initiatives were vital for the sector, as they produced definitions for issues that were not specifically stated in the regulations at the time, and brought clarity to the direct marketing sector as an activity in steady expansion. We understand that the current advancement of legislation in e-commerce and personal data protection in the region has made these procedures result in "co-regulatory" rather than self-regulatory mechanisms. This is because the trust seals coexist and replicate the applicable norms in their codes of conduct, reinforcing the private sector's efforts to implement and comply with the laws in force, to the benefit of consumers. In some cases, they may go further and include technical or quality standards. In this sense, while legislation sets mandatory standards, the trust seal schemes function as a practical interpretative guide for their implementation and enforcement. In addition, the seals, as mentioned above, serve as evidence of the fulfillment of the regulations to build trust as a marketing strategy and boost customer loyalty. Finally, they can shed light on situations not contemplated by the guidelines considering that they are dynamic industries undergoing rapid and constant technological change.

Another interesting and innovative idea is the trust seal issued by the Mexican government's Federal Consumer Protection Agency (hereinafter "Profeco"), which offers its Distintivo Digital. The purpose is to serve as an official recognition granted to those companies providing goods or services that stand out for favoring high standards in electronic commerce, such as

clear and complete information, security, transparency, confidentiality, trust, and legal certainty for the consumer. Profeco's Distintivo Digital scheme allows each member company to draw up its own Code of Ethics, which can be downloaded from the Distintivo Digital website. The Code of Ethics, as described, "is a set of values and principles that every adhering supplier must observe in activities related to electronic commerce, in order to respect and promote consumers' rights, foster a culture of responsible consumption, the protection of vulnerable groups, and self-regulation." (82)

To sum up, it is an array of minimum standards that member companies voluntarily agree to meet so that online purchases on their sites are made "within a framework of respect for consumers' rights, adopting tools and the best commercial practices at a global level." (83) The code will contain minimum criteria deemed as certification requirements, among which we highlight: information about the treatment that will be given to the personal data submitted by consumers through the Privacy Notice; concerns associated with the protection of children and adolescents; protection of vulnerable groups; furtherance of specific and alternative mechanisms for conflict and doubt resolution, requiring to act diligently in conciliatory procedures to reach agreements that benefit consumers; and implementation of strategies by the company to verify compliance with the provisions of the code (84).

It is interesting to note that the process of certification implies a check-up by Profeco to verify if the applicants' websites comply with the Distintivo Digital scheme's requirements. This includes allowing the agency to make observations and demand the correction of any deficiency detected before conceding enlistment on the Distintivo Digital site.

Finally, these types of processes known as "co-regulation", in which both companies and government participate, lead us to consider if a similar strategy could be implemented in cross-border e-commerce to encourage respect for the norms and help build trust. In particular, it could ensure a cross-border data flow in compliance with basic consumer rights and personal data protection guidelines. For example, it could be envisaged that having the States parties

instituted minimum data security requirements, certification entities could then be in a position to corroborate that businesses voluntarily adhering to the such framework are conformant. In addition, these companies could even decide to raise the standards for the benefit of their clients and their brand image. Through the trust seal, the norms are made visible to companies and users and help to build up confidence and loyalty, which, as previously said, is essential to the development of electronic commerce in the region.

All of the above is complemented by the current regulatory trend in personal data protection, which recognizes the ability of private parties to establish frameworks that conform to the norms required by law under co-regulatory systems.

4. The Agreement and local norms in the States Parties (Argentina, Brazil, Paraguay, and Uruguay)

In this section, we will examine the local regulations of the States Parties in detail and compare them with the precepts set up in the Agreement. The different attributes of these norms can be summarized in the following table:

	Argentina	Brazil	Paraguay	Uruguay
Local regulations respectful of international data protection standards	✓	✓	✖	✓
Consent as a legal basis for processing	✓	✓	✓	✓
Principle of purpose limitation	✓	✓	✓	✓
Principle of data quality	✓	✓	✓	✓
Liability regime (penalties for non-compliance)	✓	✓	✖	✓
Provisions on personal data security	✓	✓	✓	✓
International data transfer regime	✓	✓	✓	✓
Appropriate legislation on direct unsolicited commercial communications	✖	✓	✖	✖

We will now examine the regulations in each of the States parties in more detail.

4.1. Argentina

The regulatory framework for personal data protection in Argentina is in line with the provisions of the Agreement, thus not requiring substantial changes should it be adopted.

Summarily speaking, the Agreement establishes obligations as to the laws protecting data security in the following points: (i) impart norms in compliance with international standards, containing general principles such as prior consent, purpose limitation, quality, security, and responsibility, among others; (ii) security measures; (iii) international data transfers; and (iv) unsolicited direct commercial communications.

The following is a more detailed analysis of each of these issues:

4.1.1. Norms in compliance with international standards, including general principles such as consent, purpose, quality, security, and accountability, among others

In Argentina, data protection is mainly regulated by the Personal Data Protection Law No. 25,326 (hereinafter "LPDPA"), its Regulatory Decree 1558/2001, all its complementary provisions, as well as that issued by the enforcement authority (currently, the Agency for Access to Public Information and before the entry into force of Decree No. 899/2017, the National Directorate for the Protection of Personal Data).

The LPDPA expresses, under its Chapter II, the general principles relating to the data protection that govern its processing, namely, (i) lawfulness; (ii) data quality and purpose limitation; (iii) consent; (iv) information; (v) category of data; (vi) health data; (vi) data security; (vii) confidentiality; (viii) data transfer; and (ix) cross-border data transfer.

The principle of lawfulness requires controllers to register databases with the enforcement authority, which must be handled per the law and not be

intended for purposes against the rules or public morality. This obligation to register, which is not provided for by the Agreement, has been criticized for being ineffectual and the latest bills submitted discharge data controllers from that duty.[85]

The principle of data quality, laid out under LPDP Article 4, also contains that of purpose limitation, in the sense it requires, among other things, that (i) the data collected be true, adequate, relevant, and not excessive concerning the scope and purpose for which it is obtained;[86] and (ii) that the data not be used for purposes other than or incompatible with those for which they were collected [87].

Under the LPDPA, a set of obligations is established for personal data controllers and processors, including the provision for joint and several liability before the data subject in case they breach their respective obligations [88].

Finally, Argentina is still considered an Adequate Jurisdiction under European law. By this, it could be said that it fulfills the international standards referred to in the article [89]. It is worth mentioning, in this regard, that upon the entry into force of the European General Personal Data Protection Regulation (EU Regulation 2016/679), a new review was made in each jurisdiction, including Argentina, on their adequacy levels. Notwithstanding, the Agency for Access to Public Information (hereinafter "AAIP") issued different resolutions to adjust the current regulations to the European standards [90] and it is expected that, should there be any reform, the same measure will be taken to maintain the status of Adequate country.

4.1.2. Security measures

Article 9 of the LPDPA stipulates the obligation to implement security measures, declaring that the subject under such regulation "...must adopt the necessary technical and organizational measures to safeguard personal data security and confidentiality, in order to avoid its alteration, loss, unauthorized treatment or consultation, and to detect information deviations, intentional or not, whether from human or automated means" [91]. It also bans the storage and processing

of databases that do not meet integrity and security technical conditions [92]. About this point, the AAIP issued guidelines for security measures to meet this obligation through Resolution 47/2018, which, although they are not binding for the parties, can be understood as a minimum level of security to be achieved. It should be highlighted that observance of the measures will be interpreted depending on the responsible party's particular processing of the data and the state of technology at the time of its assessment.

4.1.3. Cross-border transfers

International data transfers are specially regulated under the personal data protection regime in Argentina. In principle, article 12 of the LPDPA [93] bans the transfer of personal data to jurisdictions that do not guarantee adequate levels of protection following the regulations in force [94], and the Control Authority (the AAIP) is competent to assess conformance to this standard.

However, the article then states exceptions to such prohibition, such as in the case of international treaties in which Argentina is a party [95] or when the purpose of the transfer is the cross-border cooperation between intelligence agencies in the fight against organized crime, terrorism, and drug trafficking [96], among others. In addition, Regulatory Decree 1558/2001 provides that the adequate levels of protection referred may derive from the legal order in force, self-regulatory systems, or contractual clauses providing for personal data protection. The latter two cases recognize, thus, the power of private parties to establish norms in compliance with the required standard and have been specifically regulated by the Control Authority.

Regarding self-regulatory systems, the AAIP issued Resolution 159/2018 setting up guidelines and the basic provisions to be observed in the self-regulatory scheme between companies of the same economic group, known as Binding Corporate Rules (hereinafter "BCRs") in order to meet the adequacy levels required under local regulations. [97] Should such rules diverge from the guidelines issued by the Control Authority, the transfer of data will be subject to approval by the latter.

The contractual clauses adopted by parties transferring personal data to jurisdictions that do not guarantee adequate levels of protection are regulated under Provision 60E/2016 issued by the then National Directorate for the Protection of Personal Data.[98] This Provision contains model contract clauses conceived as the minimum floor that the document to be executed between the contracting parties must guarantee, for the transfer in question. As mentioned in the case of BCRs, if the parties sign contracts differing from the approved clauses or not containing the principles, guarantees, and provisions related to personal data protection mentioned in the models, approval must be requested from the Control Authority before the transfer of the data.

4.1.4. Unsolicited direct marketing communications

In principle, the legal basis for processing personal data for advertising purposes under Argentinian law is the consent of the data subject. It must be remembered, in this regard, that article 5.1 of the Argentinian data protection norm affirms that consent must be "free, express and informed, and must be in writing or by another means that allows it to be equated according to the circumstances" and in article 5.2, enumerates the few exceptions in which consent is not required. In turn, article 6 states the obligation to inform data subjects expressly, clearly and before or at the time of collection, about the following: the purpose of the processing; the identity and address of the person responsible for the database; and the right of the data subject to access, rectify and delete. However, under the regulation of article 27 of the LPDPA, through Decree 1558/2001,[99] there appears to be an exception in which consent is waived for the collection, processing, and transfer of data used for creating profiles, which categorize individual preferences and similar behavior patterns. In such cases, subjects must be identified only by their belonging to such generic groups, with personal data management limited to the purpose of the advert. For any type of communication made by phone, post mail, e-mail, the Internet, and other remote means, the regulation establishes, first of all, that the right to request total or partial removal or blocking of the person's name from the database must be expressly and prominently indicated, i.e., the opt-out principle already referred to. The such article also stipulates that the holder can

request to be informed of the name of the person responsible for the database that provided their information. In turn, Provision 4/2009 [(100)] specifies in detail how the right of withdrawal or blocking must be informed in communications with advertising purposes. It adds that in the case of unsolicited direct marketing, the advert must be indicated as such, in its header when done through e-mail.

It is worth mentioning that under Argentinian law, the exceptions to consent by the regulations, not by the law itself, must be understood in a restrictive manner. In this sense, we deem that both the regulatory trend and the email marketing industry are moving towards opt-in schemes, i.e., those in which prior consent is required for sending adverts. In line with this, we note that the exceptions to consent for unsolicited commercial communications are restricted, as in the draft agreement between Mercosur and the European Union referred to in this paper, which only enables them in situations of prior relationship with the consumer and for selling the same type products or services.

If the Agreement enters into force, the Argentinian norm will have to be adjusted. The exception to consent provided for by Article 27 of Regulatory Decree 1558/2001 and specifically regulated by Decree 4/2009 for unsolicited direct advertising communications would no longer be valid for cases related to profiling. And instead, it should be restricted to the case in which prior relations with the consumer exist (the Agreement expressly states "within the sale of a product or service", which could create certain interpretation discrepancies as to whether such consumer must be deemed as a client, or if mentioned "sale" refers to a completed transaction or simply an offer.

4.2. Brazil

On August 1, 2021, the General Personal Data Protection Law No. 13,709, enacted on August 14, 2018 ("LGPDP") came into force in Brazil, which follows the latest regulatory trends in the field and bears similarities with the European General Personal Data Protection Regulation (EU Regulation 2016/679).

4.2.1. Norms in compliance with international standards, including general principles such as consent, purpose, quality, security, and accountability, among others

The Brazilian data protection norm affirms personal data must be processed in good faith, following ten fundamental principles: purpose limitation, adequacy, necessity, free access, quality, transparency, security, prevention, non-discrimination, and accountability.

The purpose principle means processing data must be under the legitimate, specific, and explicit purpose limited to what the data subject has consented to, and any handling incompatible with that purpose is forbidden[(101)]. This is complemented by the adequacy principle, which states that the purpose must not only be duly informed to the data subject but also be appropriate to the context [(102)], and the principle of necessity (also known as the "minimization principle")[(103)]. Under the minimization principle, the data collected should be only that which is relevant, proportionate, and not excessive concerning the purpose in question.

As regards quality, the Brazilian regulation establishes that the data must be adequate, clear, relevant, and updated following the purpose of its treatment [(104)].

The LGPDP adopts the principle of accountability, which requires data controllers to be able to prove their abidance by the applicable regulation, including the effectiveness of the measures they have adopted [(105)], to the competent authority and/or third parties.

The liability scheme of data processing agents is regulated under section III of Chapter VI. This section establishes remediation and compensation in the event of damage caused by non-compliance with the regulations, providing for joint and several liability of processors and controllers if the former fails to fulfill the instructions of the latter.[(106)]

Consent from the data subject is an essential condition for the legitimate processing of their data and has special regulations [(107)]. Among other requirements, consent must be given for limited purposes, being invalid if given in generic terms [(108)]. It also must be stated in writing or similar means, being the data controller responsible for proving it [(109)].

4.2.2. Security measures

Chapter VII of the LGPDP specifically regulates the obligation of security and good practices in personal data storage [(110)]. Following the security principle, data handling must be carried out under technical and administrative measures that protect the information from unauthorized access and accidental or illegal destruction, loss, alteration, transfer, or dissemination. Such measures must be in accordance with the nature of the information processed – especially if it is sensitive data –, the particular type of processing, and the state of technology.

In addition, the LGPDP empowers the control authority to establish minimum security standards to be adopted by controllers and processors in charge of personal data storage [(111)]. Finally, it should be noted that non-compliance with the security standards agreed upon is considered an assumption of liability under this regulation [(112)].

4.2.3. Cross-border transfers

International data transfers are regulated under Chapter V of the LGPDP, establishing the cases in which they are permitted. Examples of such situations, among others expressly stated by the law, are:

- Transfer is made to countries or international organizations that provide adequate levels of protection under Brazilian law;
- The data controller offers and guarantees fulfillment of the rights of data subjects and the norms. This may appear in the form of specific clauses for a particular transfer; model clauses; binding corporate rules; and/or seals, certifications, or codes of conduct;

- The data subject has given specific consent for the international transfer in question;
- The transfer is necessary for international legal cooperation between public intelligence, investigative and public prosecution offices, or following international law instruments, among other provisions expressly stated by the law;[113]

The adequate level of protection of a country or an international organization will be determined by the Application Authority, considering aspects such as the rules in force in the country of destination; the nature of the data; conformance to the general principles for personal data protection provided for in the LGPP. Besides this, it will also contemplate the adoption of security measures; the existence of judicial and institutional guarantees to ensure such rights, and other circumstances related to the transfer. Likewise, the Application Authority will be who determines the contents to be included in the mechanisms enabling international personal data transfer (model clauses, binding corporate rules; and/or seals, certifications, or codes of conduct, etc.) [114] and confirms fulfillment of such standards in the specific agreements.

4.2.4. Unsolicited direct marketing communications

In principle, unsolicited direct marketing communications are not allowed under the LGPDP, as consent is an essential requirement for legitimate data processing [115]. Therefore, the data subject must agree to receive commercial communications in the first place. Notwithstanding the above, as has been interpreted in the case of the European regulation, consent to receive these types of communications may be understood as implicit when there is a prior contractual relationship between the seller and consumer, provided that the content of the advert is related to the product or service that has been offered. [116] In this sense, current Brazilian legislation is in line with the Agreement studied in this document, so Brazil will not need to adjust its legislation once it enters into force.

4.3. Paraguay

Paraguay lacks a comprehensive personal data protection regime, being the issue currently regulated by Law No. 6534 on Personal Credit Data Protection. (117) Notwithstanding the name of the law, this norm includes provisions that include personal data understood as "information of any type, referring to legal entities or determined or determinable natural persons." (118)

4.3.1. Norms in compliance with international standards, including general principles such as consent, purpose, quality, security, and accountability, among others

Paraguay's normative framework under Law No. 6534 focuses mainly on credit data and the laws applicable to those providing services of this nature, so it may be said that should the Agreement come into being, the country will have to adjust its regulations. (119)

Consent is the legal basis for processing personal data under Paraguayan law, which in its Article 6 states: "The processing and transfer of personal data are unlawful when the data subject has not given their free, express and informed consent". In addition, it is worth mentioning that such consent must be "... express and unequivocal, in conditions that do not admit any doubts as to its granting and must be given in writing, electronically, digitally or by any other reliable means." Under the same article, there appears to be a certain reception of the purpose limitation principle, insofar as the right of the subject to be informed of the purpose for which the data is collected is recognized.

The principle of data quality is expressly included in article 7, declaring that "the personal data collected or stored must be lawful, accurate, complete, truthful and updated for the specific purpose for which it was obtained." Finally, the norm includes the obligation to implement security measures that must be "... necessary to safeguard the access and integrity of personal data, to avoid its alteration, loss, consultation, commercialization or unauthorized access." (120)

4.3.2. Unsolicited direct marketing communications

Under Article 6 of Law No. 6534, consent is enunciated as the basis for legitimate processing and no exceptions are provided, so it could be concluded, in principle, that unsolicited direct marketing communications are banned under Paraguayan regulation. However, Law No. 4868 on Electronic Commerce [(121)] expressly regulates the matter stipulating that providers may send resort to these types of calls or messages if they: (i) expressly indicate the quality of the unwanted communication; (ii) include an easy system of exclusion from the recipient list within the message, known as the right of opposition or opt-out; (iii) obtain the data without infringing the privacy rights of the recipients; and (iv) establish that the communication is not larger in extension than the maximum fixed by the Control Authority appointed by the law, being able to include complementary information about the offer in the same links [(122)].

4.3.3. Cross-border transfers

Article 21 of Law No. 6534 considers a case of infringement, "The international transfer of personal data to a recipient located in a third country or an international organization when the safeguards, requirements or exceptions outlined in this Law are not met". However, there is still no specific regulation determining criteria for determining compliance with the provisions therein.

4.4. Uruguay

The personal data protection regime in Uruguay is mainly regulated under the Personal Data Protection Law No. 18,331,[(123)] enacted on August 11, 2008 (hereinafter "LPDPU"), and its regulatory decree 414/009 [(124)]. In general, it can be said that in 2018, Uruguay undertook the modernization of its regulation on the matter aligned with European regulations, through the incorporation of specific provisions contained in Law 19,670 [(125)] that determine the application of the LPDPU, the obligation to notify security breaches, the principle of accountability, Resolution 32/020, providing criteria for appointing the head of

Personal Data Protection [(126)] and the recent ratification of Convention 108+ [(127)], among others.

4.4.1. Norms in compliance with international standards, including general principles such as consent, purpose, quality, security, and accountability, among others

TAs mentioned previously, Uruguay is modernizing its regulations on personal data protection, although it had been considered a jurisdiction with adequate legislation by Europe even before. Consequently, the law complies, in general, with the international standards referred to in the Agreement. Although Europe is reviewing such adequacy, as with Argentina, no decision has yet been issued to modify it.

The LPDPU prescribes certain principles under chapter II that must govern data handling, namely: i) value and force; ii) legality; iii) truthfulness; iv) purpose limitation; v) prior informed consent; vi) data security; vii) confidentiality; and viii) liability.[(128)]

Value and force refer to the obligation of data controllers and those involved in the processing to respect the rest of the principles and that these serve as a guide for the interpretation of the law in its application [(129)]. As regards the principle of legality, as in Argentina, it refers to the obligation to register [(130)]. The principle of truthfulness requires that the personal data collected be accurate, adequate, fair, and not excessive as to the purpose for which they were obtained [(131)]. The principle of purpose limitation, in turn, restricts the use of data only to the motive for which it was collected and that, once this purpose has been fulfilled, it must be deleted [(132)].

Article 9 of the Personal Data Protection Law establishes the legal basis for data storage is user consent, which must be given in a free, prior, informed, and express manner. However, the same article defines certain exceptions to consent, among which are data coming from public sources of information or if it's necessary for the development and fulfillment of a contractual relationship assumed by the data subject.

Article 10 of the law enshrines the principle of data security, requiring data controllers and processors to take measures to ensure the security and confidentiality of the information, in order to prevent alteration, loss, unauthorized consultation or processing, and to detect information deviations. In turn, this principle is complemented by that of confidentiality, which prohibits the disclosure of the data to third parties [(133)].

Finally, the principle of accountability is outlined in Art. 12, which provides for appropriate technical and organizational measures for the exercise of proactive responsibility.

4.4.2. Unsolicited direct marketing communications

Although consent is the legal basis by default under Uruguayan law, the wording of article 21, regulating data storage for advertising purposes, allows to send unsolicited direct commercial communications, as it provides for the processing of data " that is used for creating specific profiles for promotional, commercial or advertising reasons; or to track consumption habits, when they appear in documents accessible to the public or have been provided by the subjects themselves or obtained with their consent." As in the case of Argentina, this aspect of the local norm will need to be modified if the Agreement is approved.

4.4.3. Cross-border transfers

Article 23 of Law 18.331 expressly prohibits any kind of cross-border data transfer with countries or organizations that do not provide adequate levels of protection meeting the regional or international legal standards. However, as in Argentina and Brazil, this can be achieved by including contractual clauses that do safeguard the rights of data subjects.

In addition, the LPDPU considers certain cases in which the mentioned prohibition is disregarded, such as in cases of international judicial co-operation, transactions relating to bank or stock exchange transfers under the applicable legislation, and agreements within international treaties to which Uruguay is a party, among others.

5. The Agreement and other international instruments on personal data and the digital economy

An interesting task is to examine the Agreement as compared to other international instruments. The text simply refers to "general principles" on personal data (art. 2.5. (f), but to disclose the exact meaning of these, it is not only important to contemplate the national legislations of each States party, but also to review the content of various international instruments that govern them, such as the Council of Europe Convention No. 108 and the Data Protection Standards of the Ibero-American States.

On the other hand, the Agreement shares striking similarities with the Digital Economy Partnership Agreement ("DEPA") between Singapore, Chile, and New Zealand, which entered into force at the beginning of 2021, as well as with the Comprehensive and Progressive Agreement for Trans-Pacific Partnership ("CPTPP"). The fact that some passages of the Agreement are virtual quotes from the other two documents suggests the DEPA and the CPTPP were taken as sources.

5.1. Council of Europe Convention No. 108 for the Protection of Individuals concerning Automatic Processing of Personal Data, Strasbourg, 28.I.1981

EThe Council of Europe Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981 (hereinafter "Convention 108") has been updated by the amendment protocol known as Convention 108+. To date, the latter has been signed by 30 countries (including Argentina) [(134)] and ratified by only 13 (including Uruguay) [(135)] of the 55 that are party to Convention 108.[(136)]

At the time of publication, on July 5, 2022, the Committee on Foreign Affairs and Worship of the Argentinian Lower House of Congress issued a favorable opinion on Agreement 108+, giving way to the Committee on Constitutional Affairs for its consideration and subsequent submission to the Chamber for approval.

Convention 108 was first signed in 1981 and has played a fundamental role in harmonizing legislation on the protection of personal data in its States Parties, serving as a basis for international laws. The protocol of May 18, 2018, known as Convention 108+ sought to modernize Convention 108 and bolster its implementation. (137)

The influence of this document in the region as a model regulation is evident when reviewing its content. Firstly, it requires States Parties to have a standard that regulates data processing and incorporates principles that are replicated in the regulations scrutinized. (138)

In this sense, the convention proclaims the principle of data quality, which, as referred to in previous sections, requires that the information processed be proportionate and appropriate to the purpose for which it was collected. In the updated version of Convention 108, the principle of consent is added under the same paragraph, whereby the legitimacy for processing personal data will be the permission given by the data subject or a valid basis provided for by the law. As to consent, it is indicated that this must be free, specific, informed, and unequivocal, all terms which are found in the regulations of each of the countries studied. (139)

The obligation to implement security measures is also introduced as a principle under Convention 108, so as to prevent accidental or unauthorized destruction or loss, as well as against unauthorized access, alteration, or transfer. (140) Convention 108+ introduces the obligation to notify a security-related incident, in line with international trends in this area (141). This notification is expressly set down by Uruguayan law (142). In Argentina, it is sometimes held that the principle of good faith and Resolution AAIP 47/2018 would imply an obligation to notify security breaches.

Regarding international data transfer, Convention 108 seeks that States do not limit the cross-border data flow arbitrarily. Thus, restrictions must be founded on the legislation on personal data. In this respect, the text of the updated version is clearer, as it refers to the adequate levels of protection that must be guaranteed by the recipient, complying at least with Convention 108. (143)

We understand that Convention 108, currently in force and binding for Argentina and Uruguay, does not contradict the provisions of the Agreement on personal data protection but rather complements them, serving as a specific regulation over which it should take precedence. In addition, the Agreement refers to international standards that should be understood as those imposed by norms such as Convention 108.

5.2. Data Protection Standards of the Ibero-American States

The Ibero-American Network for the Protection of Personal Data established the Ibero-American States Data Protection Standards.(144) One of its goals is to deliver a set of common principles and rights in this area so that the member states develop compatible legislation guaranteeing the rights of individuals within their territory. In this regard, it is worth mentioning that, although they are not mandatory, their precepts are replicated in some of the legislations analyzed in this document and have even served as a guide for their updating, as in the case of Uruguay and Argentina (145).

Related to this, and since the Agreement declares that the States shall adopt regulations considering the international standards on the matter, it could be understood that these Standards will be taken into consideration when tackling this point (146).

The Standards begin by offering definitions under Chapter I, such as anonymization, consent, personal data, sensitive data, data processor, exporter, data controller, data subject, and processing. It also fixes general principles

for personal data protection under Chapter II. Both the definitions and the principles are aligned with those of the legislation in force in the countries seen in this document. However, they include precepts that are not currently included, except in Brazil, which can be said to have the most modern standard in the region. For example, the Standards regulate the rights to portability and to challenge automated decisions, the principle of proven responsibility, and privacy by design and default, among others that will be analyzed below.

5.2.1. Principles of Personal Data Protection

LThe Standards recognize the principles of legitimacy, lawfulness, fairness, transparency, purpose, proportionality, quality, accountability, security, and confidentiality. These are included in the local legislation of all the countries except for Paraguay, which has yet to update its regulations.

The principle of legitimacy forms the legal bases for data storage, which include the requirement of consent by the data subject, the need for processing to fulfill a legal obligation or execution of a contract, and the vital interest of the data subject or natural person, and the public interest, among others [(147)]. Consent is specifically regulated under the standards, as is generally the case with the legislations examined. In this sense, it should be noticed that the data controller is who must positively demonstrate that the data subject has granted consent through a clear affirmative action and that it is revocable, for which simple, agile, effective, and free mechanisms must be provided.

Lawfulness, under these Standards, refers to the fact that data must be processed in compliance with the legal provisions of each country.

Fairness requires that data should not be processed by misleading or fraudulent means. Here, we see that this principle is present in consumer regulations both at the regional level and in the norms of each country [(148)]. Along the same lines, the principle of transparency is recognized, being data controllers obliged to inform the subject on how their data will be handled [(149)]. This includes the identity of the controller, the purpose of the processing, international transfers

if any, the rights of the subject and the source from which the data has been collected if not directly from the subject. In addition, this information must be provided in an accessible form, using simple and comprehensible language to the subject.

It is worth mentioning that the standards provide for the exception of archiving, scientific and historical research, or statistics gathering, all of these in favor of the public interest. The principle of proportionality establishes that only data that is adequate, relevant, and limited to the purpose may be processed, also known as the minimization principle.

Quality refers to the obligation of the controller to take measures to keep data accurate, complete, and up to date. Furthermore, it must only be kept for the period demanded to meet the purposes for which it was originally stored, after which the information must be erased or anonymized. In this respect, controllers are mandated to guarantee the appropriate measures and techniques aimed for their final and secure deletion.

The Standards also include the principle of proven responsibility, which is provided for in the new Brazilian regulation on personal data protection, establishing that the controller must demonstrate compliance with the established principles and obligations. This includes attesting how the data will be handled to the subject and to the control authorities. About this point, best practices as defined by domestic laws, self-regulation schemes, and certification systems, among others, are listed as examples of how to fulfill this requirement [(150)], as well as the allocation of resources to implement programs and policies for personal data protection, adopt data risk management solutions, training programs, internal supervision, and monitoring schemes, and procedures for dealing with requests from data subjects, among others [(151)].

Security is another principle recognized by the Standards, stating that controllers must take the necessary administrative, physical, and technical steps in place to guarantee the confidentiality, integrity, and availability of personal data [(152)]. Factors to be considered are the state of technology, costs of

implementation, scope, context, purposes of the storage, international transfers, and the possible consequences of breaching, among other factors [153]. It is interesting to note that the Standards introduce the obligation to notify security incidents to the data subject and the control authority, providing that it would not be applicable if it can be proven that the breach is unlikely to occur and/or that it does not affect the data subjects involved in their rights and freedom [154].

The notification must contain certain minimum information, such as the nature of the incident, the data that was affected, the remedial actions, recommendations on what the data subject can do to protect their interests, and the means available for them to obtain further information [155]. As far as the controller is concerned, they must document the details of the security breach, such as the date, causes, related facts, and the corrective measures taken.

The obligation of personal data confidentiality as established in the Standards encompasses all persons and entities involved in its treatment and continues beyond the termination date of the relationship with the data owner [156].

5.2.2. Rights of the data subjects

The document recognizes the ARCO rights (access, rectification cancellation, or opposition) of personal data subjects under Chapter III [157]. In addition, it recognizes the right to portability [158], to avoid being subject to automated individual decisions [159], and to minimize the scope of data processing [160]. These rights are not mutually exclusive, i.e., the exercise of one does not prevent that of another [161].

The right of access means the subject is entitled to know and obtain a copy of which data is held by the controller, as well as other information related to the general and particular conditions of the processing [162].

The right of rectification concerns the power individuals have to request inaccurate, incomplete, or outdated personal information handed in to be corrected or completed on their request [163].

The right to erasure, which prescribes that subjects may request the cancellation or deletion of their data, is regulated under point 27 of the Standards and implies that the holder has no longer the right the handle their personal information [(164)].

The right to object to a processing operation is also specified in the Standards, indicating that it may be requested when (i) there is a legitimate reason or (ii) it is done for direct marketing communications (including profiling) [(165)].

The right not to be subject to automated decision-making processes is becoming increasingly relevant in times of big data and artificial intelligence and accords with the European regulations on the matter. By recognizing this right, the Standards limit automated decisions – those made without human intervention – that produce legal effects or significantly affect individuals and that aim to evaluate, analyze or predict their professional performance, economic situation, health status, sexual preferences, reliability, or behavior.

As regards automated decisions, it is relevant to note that the Standards were written in 2017 and that since then, there has been substantial progress in technology and automation. One interesting example is digital banks or Fintechs granting personal loans in the region that implement non-traditional mechanisms, involving cross-referencing and personal data-intensive processing [(166)], aiming to expand their customer portfolio. These procedures use information obtained from the traditional financial system, if there is any, plus data revealing behavior in social networks and capacity to pay, among other "digital footprints" users leave while browsing the Web. Through this, companies can combine the information with algorithms and create profiles, together with enhanced credit scoring schemes, allowing them to automatically calculate the repayment rate and determine the amount, term, and interest rate to be offered to the user in a customized way.

Although these mechanisms can serve to accelerate financial inclusion, which is a major objective in the countries in the region, it is worth asking whether these intensive segmentation, profiling, and automated scoring techniques are

in line with the standards under analysis. Similar questions arise in this respect to those posed when discussing intensive processing for advertising, both in terms of consent and the right not to be subject to automated decisions.

The challenge is laid down, on the one hand, considering the importance of technological development so as to provide more and better services to the population of the region, without hindering the power of SMEs to innovate and promote the knowledge-based economy. And, on the other hand, maintaining the highest standards of security, personal data protection, commercial loyalty, non-discrimination and, to sum up, respect for users' dignity and human rights [(167)].

Concerning automated decisions, the Standards relax the criterion and indicate that it will not be applicable when "... the automated processing of personal data is necessary for the conclusion or performance of a contract between the data subject and the data controller; it is authorized by the domestic law of the Ibero-American States, or it is grounded on the proven consent of the subject." [(168)] Returning to the example given above, a bank could validly grant credit based on an automated decision if it has the consent of the data subject for such processing. Nevertheless, the standards state that when automated decisions are permitted on grounds of consent or a contractual relationship, the data subject shall always have the right to request human intervention, receive an explanation of the decision made, express their point of view and challenge the decision [(169)].

The Standards take human rights guidelines into account, including express prohibitions on automated decisions when they have discriminatory effects: "The controller must not carry out automated processing of personal data that produce the effect of discriminating against data subjects on grounds of racial or ethnic origin; religious, philosophical or moral beliefs or convictions; trade union membership; political opinions; data concerning health, life, sexual preference or orientation, as well as genetic or biometric data." [(170)]

The right to portability, recognized in regulations such as the GDPR of the European Union, is included in the Standards, granting users the right to obtain

a copy of the personal data being processed. The data must be provided in a structured format that is easily readable and allows them to continue being used or be transferred to another controller [(171)]. The exercise of the portability right presents a challenge for controllers, as technology, in general, is not neutral or interoperable, i.e., they do not use the same data format and arrange it into a common or neutral system, making its compliance highly costly or prohibitive. Perhaps in this understanding, the Standards enunciate that when technically possible, the data subject may request the transfer of his data to another data controller [(172)].

Portability does not extend to data that is "...information inferred, derived, created, produced, or obtained from the analysis or processing done by the controller based on the data provided by the subject..." [(173)] It continues by clarifying, by way of example, that it does not reach data submitted to a process of personalization, recommendation, categorization, or profiling. We deem this reasonable, as this type of processing generally uses undisclosed techniques or algorithms specific to the know-how of the data controller or its service providers.

The right to restrict processing means that if an individual objects to the use given to their data or contests its accuracy, the controller must limit the processing to simple storage until it is resolved [(174)]. Likewise, a restriction may be demanded when, although the controller no longer needs a user's data for handling, the user needs it to remain stored to file a legal claim.

In order to guarantee the acknowledged rights, the Standards require data controllers to implement procedures for their exercise, while each State member is to determine the requirements, deadlines, and terms and conditions, as well as the grounds for possible exceptions, which could be related to processing for the fulfillment of state functions or compliance with a legal obligation, among other assumptions [(175)].

Although data protection is usually conceived as deriving from the very personal right to privacy, the Standards admit that relatives can exercise this

right over a deceased person's data [176]. This is a novel point since the norms examined in this article do not usually deal with this issue [177].

Finally, the document requires member states to recognize the possibility for a data subject to challenge the responses given to their requests, both before the control authorities and where appropriate, before the courts.

5.2.3. Cross-border personal data transfers

The Standards dedicate a chapter to the regulation of international data transfers, indicating the cases in which they are allowed. In line with the regulations discussed in this document, they establish that personal data may be transferred when the destination country grants adequate levels of protection, contractual clauses are signed between the parties, or any other instrument that offers sufficient guarantees. In addition, they refer to binding self-regulatory or certification procedures between the exporter and the recipient that are in accordance with the legislation in force of the jurisdictions, or if the control authority authorizes the such transfer [178].

The Standards give member states the power to impose limits to international transfers for categories of data, reasons of national or public security, public health, rights and freedoms of third parties, or other matters of public interest [179].

Regarding this point, it is worth mentioning that the Ibero-American Network for the Protection of Personal Data has recently opened a consultation process for preparing its guide for the use of contractual clauses as an alternative to conducting international data transfers. This guide includes clauses with adoption models for international transfers between controllers and processors to guarantee a minimum level of protection between member states. We understand that, if approved, it will serve to harmonize the norms for international data transfers between states, in line with a high standard of protection of the rights individuals have over their data.

5.2.4.Privacy by design and by default

The Standards call on member states to adopt proactive measures that promote the observance of their laws and increase self-regulation measures implemented by data controllers [(180)]. To this end, the concepts of privacy by design and by default were introduced [(181)]. The former refers to the thought that data controllers must consider data privacy and adherence to the norms from the design stage, i.e., the principle must be integrated from the moment the technology is created. The latter, in turn, determines that the process must contemplate that, when individuals are offered choices for how much data they share, the system complies with the strictest privacy settings by default, i.e., automatically.

Although privacy by design and by default are not expressly included as principles in the regulations examined in this document, there is progress towards adopting them in the reform projects of the region and the different guidelines issued by the control authorities of the countries. By way of example, the authorities of Argentina and Uruguay issued a Data Protection Impact Assessment guide that expressly incorporates both principles [(182)] and in the case of Uruguay, privacy by default and by design are listed as part of the exercise of the proactive accountability that data controllers must take.

5.2.5. Compliance officer

A good practice included in the Standards is the designation of a compliance officer. This requirement does not apply to all types of controllers but rather determines the cases in which it would be applicable. For example, when the controller is a government agency, when the processing involves regular and systematic monitoring of the user's conduct, or when there is a high risk for the data subjects [(183)].

5.2.6. Self-regulatory mechanisms

Self-regulation and the principle of what is known as proven responsibility prevail throughout the text and in the latest regulatory trends [(184)]. As far as

the Standards are concerned, point 40 indicates that the responsible parties may adhere to this type of self-regulatory scheme, which may even include dispute settlement procedures [185]. The latter is undoubtedly a novelty since the other regulations analyzed in this text understand the norms on this matter as of public order, and in principle do not enable this type of alternative self-regulated conflict solution.

The Standards expressly refer to codes of ethics and certification systems and their respective trust seals as self-regulatory mechanisms that contribute to compliance with and enforcement of the personal data regime [186]. It is worth mentioning that these mechanisms will be subject to validation and regulation by the public authorities [187].

5.2.7. Impact assessment

Impact assessment is a good practice [188] that many regulations, such as the European GDPR, have made mandatory. In this case, the Standards provide for its implementation when the personal data processing entails a high risk to the individuals involved. It is up to the member states to determine their content and the specific cases in which they will be mandatory [189]. As to Mercosur, and although they are recommended as a good practice in Argentina and Uruguay, only Brazil's legislation expressly incorporates impact assessments so far [190].

5.3. Digital Economy Partnership Agreement (DEPA) between Chile, New Zealand, and Singapore

The DEPA is a recently concluded agreement between Chile, New Zealand, and Singapore [191]. It is a novel form of treaty, focused on strengthening cooperation on key emerging issues in the digital economy, and promoting interoperability between the systems of the signatory countries. It is inherently related to the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), of which the three countries are members, and to a certain extent, the DEPA complements it, deepening its obligations within the digital

field. In addition, it is open to other members of the World Trade Organization (WTO) but so far, only Canada has shown formal interest in joining and has initiated discussions to that effect [(192)].

The DEPA addresses aspects such as encouraging end-to-end digital trade through the recognition of digital identities, electronic invoicing, paperless trade, and cooperation in fintech and electronic payment solutions. In addition, enable the flow of trusted data through protection mechanisms, international transfers, open government data, and innovation in data and regulation as well as build trust in digital systems and create opportunities for participation in the digital economy, through the adoption of an ethical framework for artificial intelligence, online consumer protection, cooperation between small and medium-sized enterprises, and the promotion of digital inclusion and participation [(193)].

It is interesting to note that the DEPA and the Mercosur Agreement have similar objectives and structures: both recognize the importance of e-commerce and the digital economy for the development of their respective countries and address various regulatory aspects with an impact on electronic transactions. However, the approach adopted by the DEPA is somewhat different from that of the Mercosur Agreement. For example, it establishes more detailed and specific obligations, resulting in a more extensive and precise agreement, while the Mercosur Agreement proposes more general obligations and standards. For example, while the Mercosur states that "each party shall endeavor to adopt measures to expedite trade conducted by electronic means" (art. 2.6), the DEPA provides for an entire module on this point (Module 2), where it refers to paperless marketing, cross-border trade logistics, electronic invoicing, express delivery and e-payments. Also, later in its text, the DEPA addresses open data, ethics in artificial intelligence, and cooperation of small and medium-sized enterprises, among other aspects, all of which are not mentioned in the Mercosur Agreement [(194)]. Finally, the DEPA institutes a specific dispute settlement system, which is not addressed in the Mercosur Agreement, perhaps due to the context of regional cooperation and the pre-existing mechanisms between the States parties on this point.

Nonetheless, the texts are strikingly similar in many aspects, including that related to the protection of personal data. In the Annex, we analyze the texts in detail. Below, we lay out a summary:

- Definition of personal data: Both agreements refer to personal data as the information belonging to an identified or identifiable natural person [(195)].
- Benefits of data protection: Both recognize the benefits of protecting personal information and its impact on increasing trust in digital commerce [(196)].
- Legal framework for the protection of personal information and international principles: Both state that each party shall adopt or maintain standards that protect e-commerce users' personal information. To this end, the DEPA indicates resorting to the "principles and guidelines of relevant international bodies", while the Agreement cites the "international standards that exist in this area". The Agreement lists some specific principles ("prior consent, purpose limitation, quality, security, accountability, among others") while the DEPA refers to others ("(a) collection limitation; (b) data quality; (c) purpose specification; (d) use limitation; (e) security safeguards; (f) transparency; (g) individual participation; and (h) accountability"). The DEPA further mentions that the regulations will consist not only of laws that broadly cover privacy, but also sector-specific norms on data protection and those that provide for the implementation of voluntary corporate commitments related to personal data protection or privacy [(197)].
- Non-discrimination principle: the DEPA stresses applying the data protection regulations in a non-discriminatory manner, while the Agreement refers to the non-discriminatory application of domestic legal frameworks for the protection of personal information [(198)].
- Release of information on personal data protection: The texts are virtually identical; both declare that the member states must provide information both for individuals to exercise their rights and for companies to comply with the norms [(199)].
- Exchange of information and sharing of experiences on data protection: Both provide for the exchange of information on the subject. The DEPA adds that this is aimed at promoting compatibility and interoperability between the parties [(200)].

- Cross-border electronic transfers: Both texts specify that the States parties recognize each may have its own regulatory requirements and allow the cross-border transfer of information for conducting business. This is done with the proviso that specific measures can be adopted in the opposite direction in order to achieve a public policy goal, provided that there is no arbitrary discrimination or a disguised restriction on trade [(201)], and the DEPA text adds that, in the latter case, the measure shall not impose restrictions on information transfers greater than those required to achieve the goal. The Mercosur Agreement, on the other hand, indicates that the article does not apply to financial services.

Other points are considered that do not deal directly with personal data protection but are related:

- Location of computer facilities: Both texts are also practically identical, declaring that one party must not require the other to use or locate computer facilities in its territory and includes exceptions for public policy goals, similar to those of the previous article [(202)]. The Mercosur Agreement adds that the article does not apply to financial services.
- Online consumer protection: The texts begin in a very similar way, stressing the importance of consumer protection in electronic commerce [(203)]. However, while the Agreement refers to the specific Mercosur norm on consumer protection [(204)], the DEPA devotes a whole chapter to particular measures, including the exploration of the benefits offered by alternative dispute resolution mechanisms.
- Principles on internet access and use: Both texts recognize the benefits of consumers being able to access and use services and applications available on the internet, connect to the devices of their choice, and be informed on network practices [(205)].

In addition, other affinities are detected, not specifically between the texts themselves but as to similar concepts and measures to be taken:

- Security mechanisms: the Agreement mentions that the parties will encourage the use of security mechanisms and data dissociation or anonymization. The DEPA, for its part, devotes a more specific chapter to

internet security [206]. Both texts expressly recognize the importance of cooperation in cybersecurity [207].

- Self-regulation, Contracts, and Trust Seals: the Agreement stipulates that the States parties will admit contract clauses or self-regulation within the private sector in order to meet an adequate level of personal data protection [208]. The DEPA, in turn, says that the parties will encourage (and not only admit) the adoption of trust seals by businesses that help verify their compliance with personal data protection standards and best practices. In addition, they will exchange information and share experiences on their use, and seek to mutually recognize each other's data protection trust seals as valid mechanisms for facilitating cross-border information transfers [209].
- While the Agreement mentions trust seals, it does so under general provisions to promote confidence and legal certainty in electronic commerce (Art. 2.5.b), along with guidelines, model contracts, and codes of conduct. The Agreement speaks of self-regulation (not necessarily through seals) and only mentions them as related to international data transfer, but not for all aspects of data protection.
- Unsolicited direct marketing communications: The Agreement seeks to effectively protect end-users against unsolicited direct marketing. To this end, it requests prior consent that will be "defined per the laws and provisions of each State party," allowing direct commercial communications within the sale of a product or service, in line with the text of the possible Mercosur-European Union agreement [210]. The DEPA, on the other hand, also commits a special chapter on this point but is stricter in this respect, even adding a point on the minimization of unwanted messages [211].

As a conclusion of this subsection, it is interesting to note the resemblance of both documents not only in their texts but also in the date of signature: the DEPA was concluded in 2020, while the Mercosur Agreement in April 2021. Perhaps the settlement date of the Agreement was linked to the halt to negotiations for a free trade agreement between Singapore and the Mercosur, which, according to some sources, occurred in mid-2020 due to the COVID-19

pandemic [212]. However, we deem it appropriate to complete the analysis with the similarities with the CPTPP, which we will see below.

5.4. Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)

The CPTPP is an agreement between Australia, Brunei Darussalam, Canada, Chile, Malaysia, Mexico, Japan, New Zealand, Peru, Singapore, and Vietnam. It is the successor to the Trans-Pacific Partnership (TPP) [213], which failed after the United States withdrew from its negotiation.

The CPTPP incorporates the text of the TPP by reference and Chapter 14 is specifically on e-commerce [214]. It contains provisions on personal data protection and other aspects of e-commerce.

A parallel with the Agreement is offered in Annex 1. Here, we highlight the following points of comparison between both texts:

- Customs duties: Art. 14.3 of the CPTPP and Art. 3 of the Agreement are substantially alike. Both texts veto the application of customs duties to cross-border electronic transmissions. However, domestic taxes, tariffs, or charges compatible with international trade agreements are accepted (WTO in the case of the Agreement and the CPTPP itself in its case).
- Electronic authentication: Art. 14.6 of the CPTPP and Art. 4 of the Agreement are almost identical. Both encourage the recognition of digital or electronic signatures from other jurisdictions and are committed to promoting interoperability in this area.
- Online consumer protection: Art. 5 of the Agreement specifically protects the online consumer, with language similar to that of Art. 14.7 of the CPTPP. While the latter includes specific provisions, the Agreement calls for MERCOSUR regulations in this regard.
- Cooperation: Art. 12 of the Agreement provides for cooperation in regulating the e-commerce sphere, similarly to Art. 14.15 of the CPTPP. Interestingly, it nearly quotes the Transpacific accord by stating that

> "the development of self-regulatory methods that promote electronic commerce by the private sector, including codes of conduct, model contracts, guidelines, and compliance mechanisms" will be encouraged. As regards the reference to self-regulation in the text, we understand that the text of the CPTPP – as well as in the Agreement – aims to a framework of co-regulation in which norms imposed by governments coexist with mechanisms developed by the private sector to promote training and achieve greater compliance. Both the CPTPP and the Agreement allude to legislation but leave room for the development of self-regulation by the private sector, recognizing its usefulness, to a certain extent, in filling the gap between the laws and their implementation in reality.

Thus, we observe that Articles 3, 4, 5, 6, 6, 8, 9, 11, and 12 of the Mercosur Agreement have their direct source in the equivalent articles of the CPTPP and that many of them served, in turn, as a reference for the DEPA and the free trade agreements between Argentina and Chile and Uruguay and Chile. It is noteworthy to mention that the Agreement has been subjected, to a large extent, to the same criticisms that these treaties (especially the TPP and the CPTPP) received as to data protection, especially regarding the half-hearted nature of the commitments made.

6. Conclusions: Opportunities and challenges for personal data protection and the growth of electronic commerce in Mercosur

As a conclusion to this paper, we highlight three aspects in the analysis of opportunities and challenges for personal data protection and the growth of e-commerce in the Mercosur area:

6.1. The impact of the Agreement on the domestic laws of the States parties: Argentina, Paraguay, and Uruguay, and their need to adjust their local data protection norms

First, the Agreement lays out a general framework for the development of data protection norms within each of the Mercosur countries: Argentina, Brazil, Paraguay, and Uruguay. In general, we see that its provisions on international standards and general principles regarding the protection of personal data follow the regulatory trend in this area. Thus, the Agreement is, to a certain extent, useful for harmonizing and promoting an updating of the different legislations, which is taking place unevenly in the region, Brazil being the country that leads the way. The signature of the Agreement itself is a significant event for the Mercosur bloc, expressing the will of its member states to foster the steady expansion of electronic commerce and to do so by respecting consumers' rights and protecting their data. However, the Agreement is somewhat lukewarm as to the latter.

Considering each State Party in particular, we note that the personal data protection laws in force in Argentina and Uruguay are in line with the standards of the Agreement so that if the Agreement enters into force, the impact should not be significant. Notwithstanding the above, Argentina, Uruguay, and

Paraguay will have to adapt the regulations governing unsolicited commercial communications for marketing purposes (art. 10 of the Agreement, inspired by art. 48 of the Mercosur - European Union agreement's negotiated text). Concerning this point, it should be expressly stated that, in principle, these communications are forbidden and that the only case enabling them is that which occurs in the context of a previous relationship ("sale of a product or service") provided that the message is related to similar products or services.

As regards Paraguay, the challenge of reaching the standard proposed by the Agreement in terms of personal data protection will be greater than for the rest of the countries. This jurisdiction will have to redesign its regulatory scheme to align it with international standards and treat the processing of personal data from a comprehensive perspective, not only restricted to credit data, expressly including principles such as purpose limitation and accountability, as well as international data transfers, among other points. Regarding Brazil, we have observed that the entry into force will not have a major impact on its norms, since its current legislation is among the most modern in the region and is fully following the provisions of the Agreement.

It is noteworthy to point out that regulatory convergence in the Mercosur countries is indeed being driven by a free trade agreement [(215)].

6.2. Similarity between the text of the Agreement and other international trade treaties: a valuable reason for Mercosur to resume international negotiations with the European Union and the CPTPP countries

Secondly, the Agreement certainly shares parallels with other international trade agreements, such as the texts of the DEPA, the CPTPP, and the free trade agreements between Argentina and Chile, and Uruguay and Chile. While the texts are in harmony with domestic laws and others that apply to all or some of the States parties (such as Convention 108 and the Iberoamerican Standards),

the question arises as to why Mercosur is concluding this Agreement. Why choose this text and why now? One possible explanation is the intention of the bloc to position itself on the international e-commerce scene with the European Union and Pacific Rim countries, especially after negotiations for trade agreements (e.g., with the European Union and Singapore) were halted only a few months before the Covid-19 pandemic. Mexico, Chile, and Peru are members of the CPTPP, although this treaty is currently in force only in the first of these countries mentioned. It is likely that Mercosur members are interested in following in the footsteps of these countries to bolster international trade, especially once the Argentina-Chile and Uruguay-Chile free trade agreements are in force.

Regarding the CPTPP and the DEPA, the main source of the Mercosur Agreement, the truth is that both treaties are very recent, and the impact adopting foreign regulations will have on the bloc remains to be seen. We deem that the Mercosur Agreement is somewhat more limited and concise than the other texts. It seems to be, at some point, a modest proposal to adopt international norms, aiming to establish similar standards and coincide with the spirit of the Pacific countries' accord, but without requiring radical changes in the local legislations of each member state [(216)].

Should Mercosur adopt norms similar to those expressed by the CPTPP and the DEPA, it faces the risk of being criticized for the same reasons: that these agreements with overly lax commitments will consolidate the market dominance of large tech companies while limiting the ability of governments to address several regulatory challenges, which, in turn, fail to bridge the digital trade gap between developed and developing countries, and offering only empty promises of dialogue on the issues such as small and medium-sized enterprises (SMEs), indigenous peoples, vulnerable groups, women and marginalized communities [(217)].These are agreements that, although they succeed in addressing important questions, are under certain criticism for being too moderate in their specific regulation, posing a lost opportunity to assume bolder commitments, together with minimum substantive requirements of respect for personal data protection and privacy as fundamental human rights.

6.3. The promotion of electronic commerce and co-regulation and their likely benefits to personal data protection, privacy, and human rights in the region

Thirdly, as regards the development of a type of e-commerce that respects the protection of personal data, privacy, and human rights, we note that the Agreement lays interesting foundations for promoting the growth of the digital economy and e-commerce in the region. However, this progress is affected by other factors (e.g., tax and customs regimes, among others) with a direct impact that should be taken into account, but are beyond the scope of this paper. Nevertheless, we believe that the path toward regulatory harmonization in e-commerce and data protection that the Agreement has undertaken will foster the development of a healthy and thriving digital economy within the region.

Finally, and considering that the Agreement makes reference to the promotion of self-regulation methods and that such a concept is taken cautiously when referring to human rights, we understand that its inclusion is appropriate in this context since they are mechanisms that complement the current norms and the jurisdictional means of enforcement, forwarding, in fact, a scheme of co-regulation in the specific areas of digital commerce and personal data protection.

As we have outlined in the background section, we are in a region where the major drivers of economic growth are SMEs, who have been turning to online channels year after year, albeit not as hastily as in developed countries. This trend sped up dramatically with the Covid-19 pandemic, leading the area to be the fastest growing in the world. This scenario implies an accelerated race to the training and professionalization of human resources, considering that the supply side (companies selling products and services online) needs to catch up in order to comply with regulations, as well as the commercial, technical and legal standards of the industry, and thus be able to successfully and respectfully manage their e-commerce activities.

Considering the above, we believe that self-regulatory tools (such as trust seals and associated codes of conduct), as a whole and as a complement to government regulation, provide SMEs with a simplified roadmap for understanding and complying with applicable norms, safety, and transparency standards, and industry best practices. In addition, they foster consumer confidence, so necessary in cross-border trade.

Thus, various co-regulation schemes provide solutions that stand out for their emphasis on consumer rights and personal data protection, and function as training, dissemination, and awareness-raising mechanisms to achieve operability and the application of best practices. All of this has a positive impact on both the public and private actors involved and is beneficial for the respect for the consumer and user rights in the region, always regarding these methods as a complement to the regulations and jurisdictional means of enforcement and not as their substitute.

We cannot fail to mention the example of Profeco's Digital Distinctive, described above, as a successful co-regulation scheme.

Finally, the promotion of these co-regulation schemes including trust seals, codes of conduct, and other procedures of the sort is not only appropriate but should be encouraged and deepened in our region due to their ability to achieve adherence and operability within the current regulations. All this in such a way as to take advantage of its potential through public-private projects aimed at addressing issues such as international data transfer, consumer protection, given the intensive use of profiling technologies in the advertising industry and online marketing, and the inclusion of vulnerable populations in the digital sphere, among many others.

7. Annex: Comparison between similar texts of the Mercosur Agreement, the DEPA and the CPTPP

Articles 3, 4, 5, 6, 8, 9, 10, 11 and 12 of the Mercosur Agreement find their direct source in equivalent articles of the CPTPP.

Articles 5, 6, 7, 8, 8, 9, 10 and 11 of the Mercosur Agreement find their direct source in equivalent articles of the DEPA (which in some cases, such as Articles 6 and 9, is also inspired by the CPTPP). Articles 2 and 12 of the Agreement, although not so similar in their wording, contain precepts related to the DEPA.

	Mercosur Agreement	DEPA	CPTPP
Customs duties	Art. 3: "1. No Party shall impose customs duties on electronic transmissions between a person of a Party and a person of another Party. 2. For greater certainty, paragraph 1 shall not prevent a Party from imposing internal taxes, fees or other charges on electronic transmissions, provided that such taxes, fees or charges are imposed in a manner consistent with the World Trade Organization (WTO) Agreements."	-	Art. 14.3: "1. No Party may apply customs duties to electronic transmissions, including electronically transmitted content, between a person of a Party and a person of another Party. 2. For greater certainty, nothing in paragraph 1 shall prevent a Party from imposing internal taxes, fees or other charges on electronically transmitted content, provided that such taxes, fees or charges are imposed in a manner that is consistent with this Agreement."

Authentication	Art. 4: "1. A Party shall not deny the legal validity of a signature solely on the grounds that it is made by electronic means, except as otherwise expressly provided in its respective legal system. 2. No Party shall adopt or maintain measures on electronic authentication that: (a) prohibit the parties to an electronic transaction from mutually determining the appropriate authentication methods for that transaction; or (b) prevent the parties to an electronic transaction from having the opportunity to prove in judicial or administrative proceedings that their transaction complies with any legal authentication requirement. 3. Notwithstanding paragraph 2, a Party may require, for a particular category of transactions, that the authentication method meet certain performance standards or be certified by an authority accredited under its legal system. 4. The Parties shall encourage the interoperable use of advanced electronic signatures or digital signatures. 5. The Parties shall provide the necessary means for the conclusion of mutual recognition agreements for advanced electronic or digital signatures."	-	Art. 14.6: "1. Except in circumstances otherwise provided for in its law, a Party may not deny the legal validity of a signature solely on the grounds that the signature is in electronic form. 2. No Party shall adopt or maintain measures on electronic authentication that: (a) prohibit the parties to an electronic transaction from mutually determining the appropriate authentication methods for that transaction; or (b) prevent the parties to an electronic transaction from having the opportunity to prove to a judicial or administrative body that the electronic transaction complies with any legal requirement for authentication 3. Notwithstanding paragraph 2, a Party may require, for a given category of transactions, that its method of authentication meet certain performance standards or that it be certified by an accredited authority 4. The Parties shall encourage the use of electronic authentication interoperability."

Online Consumer Protection	Art. 5: "The Parties recognize the importance of protecting consumers from fraudulent and deceptive commercial practices when participating in electronic commerce. In this sense, each Party shall comply, as regards consumer protection in electronic commerce, with the provisions of the Mercosur regulations in force related to the matter."	Art. 6.3: "The Parties recognize the importance of transparent and effective measures to protect consumers from fraudulent, misleading and deceptive commercial practices when engaging in electronic commerce."	Art. 14.7: "1. The Parties recognize the importance of adopting and maintaining transparent and effective measures to protect consumers from fraudulent and deceptive commercial practices such as those referred to in Article 16.7.2 (Consumer Protection) when engaging in electronic commerce. 2. Each Party shall adopt or maintain consumer protection laws to prohibit fraudulent and deceptive commercial activities that cause harm or potential harm to consumers who engage in commercial activities online. 3. The Parties recognize the importance of cooperation between their respective consumer protection agencies or relevant national bodies in activities related to cross-border electronic commerce in order to enhance consumer welfare. To this end, the Parties affirm that the cooperation sought under Article 16.7.5 and Article 16.7.6 (Consumer Protection) includes cooperation with respect to online commercial activities."

Benefits of protecting personal information and its impact on improving trust in digital commerce	Art. 6.1: "The Parties recognize the benefits of protecting the personal information of users of electronic commerce and the contribution this makes to enhancing consumer confidence in electronic commerce.	Art. 4.2.1: "The Parties recognize the economic and social benefits of protecting the personal information of participants in the digital economy and the importance of such protection in enhancing trust in the digital economy and the development of trade."	Art. 14.8.1 "The Parties recognize the economic and social benefits of protecting the personal information of users of electronic commerce and the contribution this makes to enhancing consumer trust in electronic commerce."
Legal framework for the protection of personal information, international principles	Art. 6.2: "The Parties shall adopt or maintain laws, regulations or administrative measures for the protection of personal information of users participating in electronic commerce. For such purposes, they shall consider the **international standards** that exist in this area, as provided in Article 2.5(f) Art. 2.5(f): "ensure the security of users of electronic commerce, as well as their right to the protection of personal data". Art. 2.5.(f) - Footnote 1: "For greater certainty, the Parties understand that the collection, processing and storage of personal data shall be carried out following general principles such as prior consent, purpose, quality, security, accountability, among others."	Art. 4.2.2: "To this end, each Party shall adopt or maintain a legal framework providing for the protection of personal information of users of electronic and digital commerce. At the development of its legal framework for the protection of personal information, each Party shall consider **the principles and guidelines of relevant international bodies**." Art. 4.2.2 - Footnote 1: "For greater certainty, a Party may comply with the obligation in this paragraph by adopting or maintaining measures such as **laws that broadly cover privacy**, personal information or personal data protection, **sector-specific laws** on personal data protection or privacy, or **laws that provide for the implementation of voluntary corporate commitments** related to personal data protection or privacy."	Art. 14.8.2 "To this end, each Party shall adopt or maintain a legal framework for the protection of personal information of users of electronic commerce. In developing its legal framework for the protection of personal information, each Party shall consider the principles and guidelines of relevant international organizations. Art. 14.8.2 - Footnote 6: For greater certainty, a Party may comply with the obligation in this paragraph by adopting or maintaining measures such as comprehensive privacy, personal information or personal information protection laws, **sectoral privacy laws, or laws providing for the exercise of voluntary privacy-related undertakings** by enterprises."

		Art. 4.2.3. "The parties recognize that the principles underpinning a robust legal framework for the protection of personal information should include: (a) collection limitation; (b) data quality; (c) purpose specification; (d) use limitation; (e) security safeguards; (f) transparency;(g) individual participation; and (h) accountability."	
Non-discriminatory application	Art. 6.3: "Each Party shall make efforts to ensure that its domestic legislation for the protection of electronic commerce users' personal data is applied in a non-discriminatory manner".	Art. 4.2.4: "Each Party shall adopt non-discriminatory practices in the protection of electronic commerce users from personal data breaches occurring within its jurisdiction".	Art. 14.8.3 "Each Party shall endeavor to adopt non-discriminatory practices in protecting users of electronic commerce from breaches of the protection of personal data occurring within its jurisdiction."
Information on rights and obligations related to personal data protection	Art. 6.4: "Each Party shall publish information on the protection of personal data it provides to users of electronic commerce, including how: (a) individuals may exercise their rights of access, rectification and erasure; and (b) businesses may comply with any legal requirements."	Art. 4.2.5: "Each Party shall publish information on the protection of personal data it provides to electronic commerce users, including how: (a) individuals may make complaints; and (b) businesses may comply with any legal requirements."	Art. 14.8.4 "Each Party shall publish information regarding the protection of personal data it provides to electronic commerce users, including the manner in which: (a) individuals may take action; and (b) businesses may comply with any legal requirements."
Exchange of information and experiences in data protection	Art. 6.5: "The Parties shall exchange information and experiences regarding their personal data protection laws."	Art. 4.2.7: "The Parties shall exchange information on how the mechanisms referred to in paragraph 6 apply to their respective jurisdictions and explore ways to extend these or other appropriate arrangements to	Art. 14.8.5 "Recognizing that Parties may have different legal approaches to protecting personal information, each Party should encourage the development of procedures that promote compatibility

		promote compatibility and interoperability between them."	between their different regimes. These procedures may include recognition of regulatory outcomes, either autonomously or by mutual agreement, or of broader international frameworks. To this end, the Parties shall endeavor to exchange information on any such mechanisms applied in their jurisdictions and explore ways to expand these or other appropriate means to promote compatibility between them."
Cross-border transfer electronic data transfer	Art. 7: "1. The Parties recognize that each Party may have its own regulatory requirements on the transfer of information by electronic means, including that with regarding the protection of personal data, as set out in Article 6. 2. Each Party shall permit the cross-border transfer of information by electronic means where this activity is a business transaction of a person from the Party. For greater certainty this paragraph shall be subject to compliance with the provisions of Article 6.7 3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure is not	Art. 4.3: "The Parties affirm their level of commitments regarding the cross-border transfer of data by electronic means, in particular, but not exclusively: 1. The Parties recognize that each Party may have its own regulatory requirements on the transfer of information by electronic means. 2. Each Party shall permit the cross-border transfer of information by electronic means, including personal data, where such activity is for business transaction of a covered person. 3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner	Art. 14.11 "The Parties recognize that each Party may have its own regulatory requirements relating to the transfer of data by electronic means. 2. A Party shall permit cross-border transfers of information by electronic means, including personal data, where such activity is s business transaction of a covered person. 3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner that would imply arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on transfers of information

	applied in a manner that would imply arbitrary or unjustifiable discrimination or a disguised restriction on trade. 4. This Article does not apply to financial services."	that would imply arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on transfers of information greater than those required to achieve the objective.'"	greater than those required to achieve the objective."
Location of computer facilities	Art. 8: "1. The Parties recognize that each Party may have its own regulations on the use of computer facilities, including requirements that seek to ensure the security and confidentiality of communications. 2. A Party may not require a person of another Party to use or locate computer facilities in the territory of that Party as a condition for the conduct of business in that territory. 3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure is not applied in a manner that would imply a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade. 4. The Parties recognize that using or locating the computer facilities in which they house personal data transferred under the Agreement outside their	Art. 4.4.: "The Parties affirm their level of commitments regarding the location of computer facilities, in particular, but not exclusively: "1. The Parties recognize that each Party may have its own regulations on the use of computer facilities, including requirements that seek to ensure the security and confidentiality of communications. 2. No Party may require a covered person to use or locate computer facilities in the territory of that Party as a condition for the conduct of business in that territory. 3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner that would imply a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on the use or location	Art. 14. 13 1. The Parties recognize that each Party may have its own regulations on the use of computer facilities, including requirements that seek to ensure the security and confidentiality of communications. 2. No Party may require a covered person to use or locate computer facilities in the territory of that Party as a condition for the conduct of its business in that territory. 3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 1 to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner that would imply a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on the use or location of computer facilities greater than those required to achieve the objective.

	territory implies an international transfer, in the terms of Article 7. 5. This Article does not apply to financial services."	of computer facilities greater than those required to achieve the objective."	
Principles on Internet access and use	Art. 9: "The Parties recognize the benefits of consumers in their territories having the ability to: (a) access and use the services and applications of their choice available on Internet 2; (b) connect end-user devices of their choice to the Internet, subject to each Party's technical regulations; and (c) access information about the network practices of the Internet service provider that may influence the consumer's decision."	Art. 6.4: "Subject to applicable policies, laws and regulations, the Parties recognize the benefits of their consumers having the ability to: (a) access and use services and applications of the consumer's choice available on the Internet, subject to reasonable network management; (b) connect end-user devices of the consumer's choice to the Internet, provided that such devices do not harm the network; and (c) access information about the network management practices of the consumer's Internet access service provider."	Art. 14.10 "Subject to applicable policies, laws and regulations, the Parties recognize the benefits of consumers in their territories having the ability to: (a) access and use services and applications of their choice available on the Internet, subject to reasonable network management 7 ; (b) connect end-user devices of their choice to the Internet, provided that such devices do not harm the network; and (c) access information on network management practices of consumer Internet access service providers."
Cooperation	Art. 12. "Recognizing the global nature of electronic commerce, the Parties affirm the importance of: (a) working together to facilitate the use of electronic commerce, generate best practices to enhance the capabilities to conduct business, collaborate and cooperate on technical and assistance issues to maximize opportunities for micro, small and medium-sized enterprises;	(non-equivalent text)	Art. 14. 15: "Recognizing the global nature of electronic commerce, the Parties shall endeavor to: (a) work together to support micro, small and medium-sized enterprises in overcoming obstacles to its use; (b) share information and experiences on regulations, policies, enforcement and compliance relating to electronic commerce, including:

	(b) share information and experiences on laws, regulations, policies, and programs in the field of electronic commerce, including those related to the protection of personal information; consumer protection, security in electronic communications, recognition and facilitation of the interoperability of cross-border electronic signatures, including advanced electronic signatures or digital signatures, electronic authentication, server location, intellectual property rights, electronic government, and initiatives for the promotion and dissemination of access to and use of electronic commerce by micro, small, and medium-sized enterprises; (c) exchange information and share views on consumer access to products and services offered online among the Parties; (d) actively participate in regional and multilateral fora to promote the development of electronic commerce; (e) **encourage the development by the private sector of self-regulatory methods that promote electronic commerce, including codes of conduct, model contracts, guidelines, and compliance mechanisms; [. ..]**		(i) protection of personal information; (ii) online consumer protection including means of consumer means of consumer retribution and enhancing consumer confidence; (iii) unsolicited commercial electronic messages;(iv) security in electronic communications; (v) authentication; and (vi) e-government; (c) exchange information and share views on consumer access to products and services offered online among the Parties; (d) actively participate in regional and multilateral fora to promote the development of electronic commerce; and (e) promote the development by the private sector of self-regulatory methods that encourage electronic commerce, including codes of conduct, model contracts, guidelines, and enforcement mechanisms.“

8. Notas

(1) It should be stressed that to the date of completion of this paper (June 2022), the Agreement has not yet entered into force. According to its Article 14, the document will be effective thirty (30) days after the second Mercosur State Party deposits its instrument of ratification. So far, only Uruguay has done so https://www.mercosur.int/documento/acuerdo-sobre-comercio-electronico-del-mercosur/

(2) Agreement, Art. 5

(3) Agreement, Art. 8

(4) Agreement, Art. 2

(5) For the purpose of this paper, we will use the terms e-commerce and digital trade interchangeably, using the definition provided by the World Trade Organization: "the production, distribution, marketing, sale or delivery of goods and services by electronic means". For more information on the definition, please consult the following link: https://www.wto.org/english/thewto_e/minist_e/mc11_e/briefing_notes_e/bfecom_e.htm#:~:text=Electronic%20commerce%2C%20or%20e%2Dcommerce,other%20public%20or%20private%20organizations

(6) Mateo Ceurvels, "Latin America Ecommerce Forecast 2021", Insider Intelligence, eMarketers, July 2021, available at https://www.emarketer.com/content/latin-america-ecommerce-forecast-2021, p.1

(7) S. Herreros, "Cross-border e-commerce regulation in trade agreements: some policy implications for Latin America and the Caribbean", International Trade series, No. 142 (LC/TS.2019/42), Santiago, CEPAL Economic Commission for Latin America and the Caribbean, 2019, p.5

(8) In this paper, microenterprises are included within the term "SMEs".

(9) Although quantifying e-commerce poses great methodological challenges and the available statistics are often not comparable, estimates suggest that has this type of trade been increasing year after year in Mercosur countries. For more information on the subject, from both the supply and demand sides, we refer to the annual reports of the Argentinian Chamber of Electronic Commerce, at https://www.cace.org.ar/estadisticas, for Brazil, at https://www.ebit.com.br/webshoppers, for Paraguay https://www.capace.org.py/blog/categories/estadisticas, and for Uruguay, to the Chamber of Digital Economy of Uruguay, at https://www.cedu.org.uy/informes

(10) Mateo Ceurvels, "Latin America Ecommerce Forecast 2021," Insider Intelligence, eMarketers, July 2021, available at https://www.emarketer.com/content/latin-america-ecommerce-forecast-2021

(11) Ibidem

(12) In the same vein, S. Herreros points out that, "Despite particularities within the countries, Latin America and the Caribbean show a considerable lag in their integration into the digital economy", in "Cross-border e-commerce regulation in trade agreements: some policy implications for Latin America and the Caribbean", International Trade series, No. 142 (LC/TS.2019/42), Santiago, CEPAL Economic Commission for Latin America and the Caribbean, 2019, p.7.

(13) "Cross-border e-commerce regulation in trade agreements: some policy implications for Latin America and the Caribbean", International Trade series, No. 142 (LC/TS.2019/42), Santiago, CEPAL Economic Commission for Latin America and the Caribbean, 2019, p.13

(14) For more information on the impact of the COVID-19 pandemic on global Electronic Commerce, we refer to the report of the United Nations Commission on International Trade Law (UNCTAD) available here https://unctad.org/system/files/official-document/tn_unctad_ict4d18_en.pdf

(15) Mateo Ceurvels, "Latin America Ecommerce Forecast 2021", Insider Intelligence, eMarketers, July 2021, available at https://www.emarketer.com/content/latin-america-ecommerce-forecast-2021. p.1

(16) Ibidem, p.2

(17) Ibidem, p.9

(18) Kantar Insights "Argentinians and eCommerce: how we sell and buy online" drafted by the Argentinian Chamber of Electronic Commerce. p.16

(19) Mateo Ceurvels, "Latin America Ecommerce Forecast 2021", Insider Intelligence, eMarketers, July 2021, available at https://www.emarketer.com/content/latin-america-ecommerce-forecast-2021. p.21

(20) Kantar Insights "Argentinians and eCommerce: how we sell and buy online" drafted by the Argentinian Chamber of Electronic Commerce. pp.150,151

(21) S. Herreros, "Cross-border e-commerce regulation in trade agreements: some policy implications for Latin America and the Caribbean", International Trade series, No. 142 (LC/TS.2019/42), Santiago, CEPAL Economic Commission for Latin America and the Caribbean, 2019, p.11

(22) Ibidem, p.13

(23) Argentina under Resolution of the Domestic Trade Secretariat of the Ministry of

Development No. 270/2020 of the MDP of 04/09/20, published in the Official Journal on 9 September 20; Brazil through Decree No. 10,271 of 6 March 2020, published in the Official Journal on 9 March 2020; Paraguay through Decree of the Presidency of the Republic No. 4053 of 15 September 2020; and Uruguay through Decree of the EP No. 167/021 of 2 June 2021, published in the Official Journal on 8 June 2021. Information available at: https://normas.mercosur.int/public/normativas/3768

(24) Ratified by Argentina and Uruguay. Entered into force on 13 August 2021, https://www.mercosur.int/acuerdo-de-reconocimiento-mutuo-de-firmas-digitales-en-el-mercosur/ and https://www.mre.gov.py/tratados/public_web/ConsultaMercosur.aspx

(25) The initiatives of this Group's Agenda are available at: https://www.mercosur.int/temas/agenda-digital/

(26) Ratified by Argentina. Entered into force in August 2021 https://www.mre.gov.py/tratados/public_web/DetallesTratado.aspx?id=o1dBpUe2l7MGQuG0qA/Cmw== , https://www.mercosur.int/acuerdo-de-reconocimiento-mutuo-de-firmas-digitales-en-el-mercosur/

(27) MERCOSUR Resolution 37/19, available at: https://normas.mercosur.int/public/normativas/3768

(28) Argentina under Resolution of the Domestic Trade Secretariat of the Ministry of Development No. 270/2020 of the MDP of 04/09/20, published in the Official Journal on 9 September 20; Brazil through Decree No. 10,271 of 6 March 2020, published in the Official Journal on 9 March 2020; Paraguay through Decree of the Presidency of the Republic No. 4053 of 15 September 2020; and Uruguay through Decree of the EP No. 167/021 of 2 June 2021, published in the Official Journal on 8 June 2021. Information available at: https://normas.mercosur.int/public/normativas/3768

(29) The text has not been ratified and is not in force, being available at the following link https://www.cancilleria.gob.ar/es/acuerdo-mercosur-ue. Subsection 6 refers to electronic commerce.

(30) Possible Mercosur-European Union Agreement, Art.42.

(31) Possible Mercosur-European Union Agreement, Art.46.

(32) Possible Mercosur-European Union Agreement, Art.47.

(33) Possible Mercosur-European Union Agreement, Art.48.

(34) Ibidem

(35) See "Chile-Uruguay Free Trade Agreement," at https://www.subrei.gob.cl/acuerdos-comerciales/acuerdos-comerciales-vigentes/uruguay

(36) See "Chile-Argentina Trade Agreement", at https://www.subrei.gob.cl/acuerdos-comerciales/acuerdos-comerciales-vigentes/argentina

(37) Agreement, Art.1

(38) Free Trade Agreement between Argentina and Chile, available at https://www.subrei.gob.cl/docs/default-source/acuerdos/argentina/texto-acuerdo-de-libre-comercio-chile-argentina.pdf?sfvrsn=da8b6d7_2, and Free Trade Agreement between Uruguay and Chile, available at https://www.subrei.gob.cl/docs/default-source/acuerdos/uruguay/texto-alc-chile-uruguay.pdf?sfvrsn=85b8e4a5_0

(39) Agreement, Art. 2.5.b, d and f respectively

(40) Argentina under Resolution of the Domestic Trade Secretariat of the Ministry of Development No. 270/2020 of the MDP of 04/09/20, published in the Official Journal on 9 September 20; Brazil through Decree No. 10,271 of 6 March 2020, published in the Official Journal on 9 March 2020; Paraguay through Decree of the Presidency of the Republic No. 4053 of 15 September 2020; and Uruguay through Decree of the EP No. 167/021 of 2 June 2021, published in the Official Journal on 8 June 2021. Information available at: https://normas.mercosur.int/public/normativas/3768

(41) Security measures and disassociation or anonymization techniques represent a challenge both for controllers responsible for compliance and the authorities who must oversee and/or audit them, in view of constant technological development. Thus, for example, security measures may become vulnerable over time or an anonymization technique which may suffice at a given moment might eventually become obsolete.

(42) Agreement, Art. 2.5b: "Considering the potential of electronic commerce as a means for social and economic development, the Parties recognize the need to: [...] (b) encourage self-regulation in the private sector to increase confidence and legal certainty in electronic commerce, respecting the interests and rights of users, through initiatives such as guidelines, model contracts, codes of conduct and trust seals."

(43) In principle, under Argentinian domestic laws there is a ban on personal data transfers to countries that do not provide adequate levels of protection (Personal Data Protection Law No. 25,326, Art. 12, states that "It is forbidden to clarifies that "(...)It is understood that a State or international organization provides an adequate level of protection when such protection is derived directly from the legal system in force, or from self-regulation systems, or from the protection established in the contractual clauses providing for personal data protection of ". In this context, the then National Directorate for the Protection of Personal Data (today under the structure of the Agency for Access to Public Information) issued Provision 60E/2016,

which provides model clauses for international data the transfer contracts of to unsuitable countries and the Agency for Access to Public Information established through Resolution 159/2018 the guidelines and basic contents of the binding corporate rules regulating such transfers. It is worth mentioning that in the event that the documents in question do not fulfill the requirements set forth in these rules, the approval of the Agency for Access to Public Information must be required prior to the transfer of personal data to jurisdictions that do not guarantee adequate levels of protection.

(44) An example of this could be the personal data sovereignty bills such as the one drafted in Argentina by legislators Sandra Mendoza, Adrián Grana, Carlos Castagneto, Eduardo Seminara, Juan Manuel Huss and Rodrigo Martín Rodríguez (File 0526-D-2017) that sought to regulate data originated from the national government, establishing that it must be stored in Argentinian territorian. Project available at: **https://www.hcdn.gob.ar/proyectos/textoCompleto.jsp?exp=0526-D-2017&tipo=LEY**

(45) Agreement, Art. 7.4

(46) CPTPP, Chapter 11, which specifically regulates the matter, and Art. 1.12 of the DEPA, excluding financial services.

(47) Personal Data Protection Law Nº25.326, Art. 12 section c, and Personal Data Protection Law 18,331, Art.23, section 3

(48) Personal Data Protection draft law D-2162170 in Paraguay, Art. 57. Available at **http://silpy.congreso.gov.py/expediente/123459**

(49) Agreement, Art. 8.1

(50) Agreement, Art. 8.2

(51) Agreement, Art. 8.3

(52) Ibidem

(53) Sebastián Herrero identifies the obligation to store certain data in local servers and/or develop local infrastructure for that purpose as a barrier to the growth of digital trade in the region. S. Herreros, "Cross-border e-commerce regulation in trade agreements: some policy implications for Latin America and the Caribbean", International Trade series, No. 142 (LC/TS.2019/42), Santiago, CEPAL Economic Commission for Latin America and the Caribbean, 2019. **https://repositorio.cepal.org/bitstream/handle/11362/44667/1/S1900451_es.pdf**

(54) Draft bill 0526-D-2017 submitted by legislators Sandra Mendoza, Adrián Grana, Carlos Castagneto, Eduardo Seminara, Juan Manuel Huss and Rodrigo Martín Rodríguez. Available at **https://www.hcdn.gob.ar/proyectos/resultados-buscador.html**

(55) Agreement, Art. 10.1

(56) Art. 48: "Unsolicited direct marketing communications 1. Each Party shall endeavour to protect end-users effectively against unsolicited direct marketing communications. To this end, in particular the following paragraphs shall apply. Each Party shall endeavour to ensure that natural and juridical persons do not send direct marketing communications to consumers who have not given their consent 23. Notwithstanding paragraph 2, the Parties shall allow natural and juridical persons which have collected, in accordance with each Party's own laws and regulations, a consumer's contact details in the context of the sale of a product or a service, to send direct marketing communications to that consumer for their own similar products or services. 4. Each Party shall endeavour to ensure that direct marketing communications are clearly identifiable as such, clearly disclose on whose behalf they are made, and contain the necessary information to enable end-users to request cessation free of charge and at any moment." Available at https://trade.ec.europa.eu/doclib/docs/2019/july/tradoc_158159.%20Services%20and%20Establishment.pdf

(57) Agreement, Art. 10.2

(58) Information on the above-mentioned event in its 2019 edition is available at http://emailsummit.org/2019/ while information on all editions of the event is available at http://emailsummit.org/

(59) We understand that the regulation is especially belated in ensuring the user consent to receive unsolicited direct marketing communications and in terms of compliance with the minimum standard of the right of withdrawal or blocking as a generalized, well-implemented practice. In addition, we note that the region does not seem to have adequate enforcement mechanisms for cases of non-compliance.

(60) As an example, it seems relevant to cite the following article by Michael Veale and Frederik Zuiderveen Borgesius: "Adtech and Real-Time Bidding under European Data Protection Law," 2021, German Law Journal. available at https://osf. io/preprints/socarxiv/wg8fq/ which examines the difficulty in seeking harmony between contemporary ad tech systems, which underpin much of its development by profiling users based on their behavior online through mobile apps, and the legal basis for processing, transparency and security required by the current European Data Protection Regulation (GDPR).

(61) More information on this initiative is available at https://mydata.org/

(62) De Mooy, M. (2017). Rethinking privacy self-management and data sovereignty in the age of big data: Considerations for future policy regimes in the United States and the European Union. Bertelsmann Stiftung.

(63) Agreement, Art. 12.a

(64) CMC Decision N° 37/03, which approves the Regulations of the Olivos Protocol for the Settlement of Disputes in Mercosur. The Olivos Protocol can be found at https://opil.ouplaw.com/view/10.1093/law-oxio/e148.013.1/law-oxio-e148-regGroup-1-law-oxio-e148-source.pdf

(65) Official information available in Spanish at https://www.mercosur.int/quienes-somos/solucion-controversias/

(66) De Mooy, M. (2017). Rethinking privacy self-management and data sovereignty in the age of big data: Considerations for future policy regimes in the United States and the European Union. Bertelsmann Stiftung.

(67) Ibidem

(68) Hirsch, D. D. (2010). The law and policy of online privacy: Regulation, self-regulation, or co-regulation. Seattle UL Rev., 34, 439

(69) Ibidem

(70) Ibidem

(71) Listokin, S. (2015). Industry Self-Regulation of Consumer Data Privacy and Security, 32 J. Marshall J. Info. Tech. & Privacy L. 15 (2015). The John Marshall Journal of Information Technology & Privacy Law, 32(1), 2

(72) OECD. Industry Self-Regulation: Role and Use in Supporting Consumer Interests. Organization for Economic Cooperation and Development, March 2015. cited in e Mooy, M. (2017). Rethinking privacy self-management and data sovereignty in the age of big data: Considerations for future policy regimes in the United States and the European Union. Bertelsmann Stiftung

(73) Hirsch, D. D. (2010). The law and policy of online privacy: Regulation, self-regulation, or co-regulation. Seattle UL Rev., 34, 439

(74) Ibidem

(75) De Mooy, M. (2017). Rethinking privacy self-management and data sovereignty in the age of big data: Considerations for future policy regimes in the United States and the European Union. Bertelsmann Stiftung

(76) Co-regulation refers to a control system in which government and industry participate, sharing responsibility for drafting and applying the standards. Dennis D. Hirsch describes it as a hybrid regulatory system. Hirsch, D. D. (2010). The law and policy of online privacy: Regulation, self-regulation, or co-regulation. Seattle UL Rev., 34, 439

(77) Regarding online complaints, in 2015, the Hot Sale Seal of the eConfianza program offered integration with an Online Dispute Settlement platform called Pactanda, as a pilot

test, to channel consumer complaints during the massive online shopping event called Argentina Hot Sale, organized by the Argentinian Chamber of Electronic Commerce (CACE). The results were presented at the eCommerce Day meeting 2015 held by the eCommerce Institute and the Argentinian Chamber of Electronic Commerce in the session "Good Practices and Trust Generation in the Online Channel, Case of Success of After-Sales with Hot Sale and Pactanda Seal: Casa del Audio", available at https://www.ecommerceday.org.ar/2015/presentaciones-2015/

(78) For more information on the Internet Association of MX history of the Trust Seals, visit the following https://sellosdeconfianza.org.mx/?op=que

(79) For more information on the eConfianza Regional Seals, visit https://ecommerce.institute/econfianza/ and https://fr.slideshare.net/einstituto/presentacin-sellos-econfianza-2013

(80) The outreach activities of the CACE Seals included training events for Companies of the sector, as can be seen, for example, in the event organized by the Argentinian Chamber of Electronic Commerce at the University of Palermo in April 2012, in the City of Buenos Aires, Argentina: https://www.cace.org.ar/agenda-e-commerce-seminario-abril in which trust building and electronic dispute settlement were discussed, and in the November 2013 meeting for the presentation of the Seals http://www.einstituto.org/site/2811-invitacion-desayuno-sellos-cace/ where the topics of Coding Good Practices and self-regulation on the Internet were discussed.

(81) Provision 4/2004 approving the Code of Ethics of the Direct and Interactive Marketing Association of Argentina, available at http://servicios.infoleg.gob.ar/infolegInternet/anexos/100000-104999/101360/norma.htm

(82) https://distintivodigital.profeco.gob.mx/

(83) https://distintivodigital.profeco.gob.mx/info-codigo-de-etica.php

(84) The complete list of the requirements for companies to join are listed at https://distintivodigital.profeco.gob.mx/info-codigo-de-etica.php

(85) For example, in the Bill presented by Senator Dalmacio E. Mera available at the following link: https://www.senado.gob.ar/parlamentario/comisiones/verExp/2986.20/S/PL. This law project expands on the bill drafted by the Agency for Access to Public Information in 2018, and submitted to Congress by the Executive Branch for the consultation of interested parties. Available at https://www.argentina.gob.ar/aaip/datospersonales/proyecto-ley-datos-personales

(86) LPDPA, Art. 4, Section 1

(87) LPDPA, Art. 4, Section 3

(88) LPDPA, Art. 11, Section 4

(89) Commission Resolution C (2003) 1731 dated June 30, 2003 pursuant to Directive 95/46/EC.

(90) Some examples of these regulations are Resolution N° 40/2018 regarding the Model Policy on Personal Data Protection for Public Bodies and the Personal that companies may incorporate into their self-regulatory rules (by way of binding corporate rules), among others. In addition, Argentina ratified the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981, known as "Convention 108" which will be dealt with in a specific section of this document. Data Protection Delegate; Resolution N°47/2018 on Security Measures; Resolution N° 159/2018, by which guidelines and basic contents were approved

(91) LPDPA, Art. 9, Section 1

(92) LPDPA, Art. 9, Section 2

(93) LPDPA, Art. 12, Section 1: "The transfer of any kind of personal data to countries or international or supranational organizations that do not provide adequate levels of protection is prohibited."

(94) Through Provision 60e/2016, the National Directorate of Personal Data Protection, currently included under the structure of the Agency for Access to Public Information, establishes that the countries that meet adequate levels of protection under Argentinian law are: the Member States of the European Union and members of the European Economic Area (EEA), Swiss Confederation, Guernsey, Jersey, Isle of Man, Faroe Islands, Canada only regarding its private sector, Principality of Andorra, New Zealand, Uruguay and State of Israel only regarding data that receive automated processing. This provision was amended by the Access to Public Information Agency in 2019 in order to expressly incorporate the United Kingdom of Great Britain and Northern Ireland.

(95) LPDPA, Art. 12, Section 2.d

(96) LPDPA, Art. 9, Section 2.e

(97) Agency for Access to Public Information Resolution N° 159/2018 available at **http://servicios.infoleg.gob.ar/infolegInternet/anexos/315000-319999/317228/norma.htm**

(98) Provision 60E/2016 issued by the former control authority National Directorate of Personal Data Protection, now named the Agency for Access to Public Information (AAIP) **http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/norma.htm**

(99) Regulatory Decree of Law 25,326 N°1558/2001, available at **http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70368/norma.htm**

(100) Provision 4/2009 issued by the former control authority National Directorate of Personal Data Protection, now named the Agency for Access to Public Information (AAIP), available at https://www.argentina.gob.ar/normativa/nacional/disposici%C3%B3n-4-2009-151221/texto

(101) LGPDP, Art. 6. I

(102) LGPDP, Art. 6. II

(103) LGPDP, Art. 6. III

(104) LGPDP, Art. 6. V

(105) LGPDP, Art. 6. X

(106) LGPDP, Art. 42. 1. I

(107) LGPDP, Art. 7. I

(108) LGPDP, Art. 8. 4

(109) LGPDP, Art. 8. 2

(110) LGPDP, Art. 6. VII

(111) LGPDP, Arts. 40, 46 and 49

(112) LGPDP, Art. 44

(113) LGPDP, Art. 33

(114) LGPDP, Art. 35

(115) LGPDP, Art. 7

(116) Information Commissioner's Office. Privacy and Electronic Communications Regulations. Direct Marketing. https://ico.org.uk/media/1555/direct-marketing-guidance.pdf

(117) Law No. 6534, available at https://www.bacn.gov.py/leyes-paraguayas/9417/ley-n-6534-de-proteccion-de-datos-personales-crediticios

(118) Law No. 6534. Art. 3

(119) In this regard, it is worth mentioning that draft laws have been presented that would seek to align the regulation of personal data protection with the European standard. http://www.diputados.gov.py/index.php/noticias/presentan-proyecto-de-ley-que-garantizara-la-proteccion-de-los-datos-personales-en-nuestro-pais

(120) Law No. 6534, Art. 10

(121) Law No. 4868. Text available at https://www.bacn.gov.py/leyes-paraguayas/961/ley-n-4868-comercio-electronico

(122) Law Nº 4868, Art. 23

(123) Law Nº 18,331. Available at https://www.impo.com.uy/bases/leyes/18331-2008

(124) Regulatory Decree 414/009. Available at https://www.impo.com.uy/bases/leyes/18331-2008

(125) Law 19,670 adopts specific provisions on personal data protection in its Articles 37 to 40. Text Available at: https://legislativo.parlamento.gub.uy/htmlstat/pl/leyes/Ley19670.pdf. It is worth mentioning that Regulatory Decree No. 64/020 expressly refers that the norm draws upon "European Regulation No. 2016/679 on the protection of natural persons in relation to the processing and the free movement of their personal data, the Standards on Personal Data Protection of the Ibero-American Data Protection Network issued in June 2017, the Council of Europe Convention No. 108 for the Protection of Individuals regarding Automatic Processing of Personal Data, its Additional Protocol of November 8, 2001 – both approved by Law No. 19,030 of December 27, 2012 – and the Protocol for Updating of the said Convention approved by the Council of Europe Committee of Ministers on May 18, 2018, signed by the Oriental Republic of Uruguay on October 10, 2018", Text available at: https://www.impo.com.uy/bases/decretos/64-2020

(126) Resolution 32/2020 of the Regulatory and Personal Data Control Unit. Available at: https://www.gub.uy/unidad-reguladora-control-datos-personales/sites/unidad-reguladora-control-datos-personales/files/2020-05/Resoluci%C3%B3n%2032-%202020.pdf

(127) Official Information available at: https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/noticias/uruguay-ratifico-convencion-108-modernizada#:~:text=Uruguay%20is%20the%20first%20pa%C3%ADs,Datos%20Personales%20(Convenio%20108%2B)

(128) LPDPU, Chapter II

(129) LPDPU, Art. 5

(130) LPDPU, Art. 6

(131) LPDPU, Art. 7

(132) LPDPU, Art. 8

(133) LPDPU, Art. 11

(134) Argentina ratified it through Law 27,483.

(135) Countries ratifying it are available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?module=treaty-detail&treatynum=223

(136) States Parties to Convention 108 are enlisted at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?module=signatures-by-treaty&treatynum=108

(137) The comparative table which appears on the official website highlights the differences between one text and the other: https://rm.coe.int/cahdata-convention-108-table-e-april2018/16808ac958

(138) Convention 108, Art. 4

(139) Convention 108, Art. 5

(140) Convention 108, Art. 7

(141) Convention 108, Art. 7.1

(142) Law 19,670, Art. 38

(143) Convention 108+, Art. 14

(144) Ibero-American Network for the Protection of Personal Data. Personal Data Protection Standards. Available at https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

(145) In Uruguay, Law 19,670, which introduces amendments to the LPDPU, expressly refers to these standards as a source, and the same happens with the law reform projects in Argentina cited in this document.

(146) Agreement 6.2.: "The Parties shall adopt or maintain laws, regulations or administrative measures for the protection of the personal information of users participating in electronic commerce. For such purposes they shall consider the international standards existing in this area, as provided in Article 2.5(f).

(147) Chapter II, Item 11

(148) Item 15

(149) Item 16

(150) Item 20

(151) Item 20.3

(152) Item 21.1

(153) Item 21.2

(154) Items 22.1 and 22.2

(155) Item 22.4

(156) Item 23

(157) Item 24

(158) Items 24 and 30

(159) Item 29

(160) Item 31

(161) Item 24.2

(162) Item 25

(163) Item 26

(164) Item 27

(165) Item 28

(166) This type of technology is essential to increase financial inclusion in countries where a large segment of their population have no credit in the traditional banking system and do not qualify for loans.

(167) For some examples of the activities carried out by digital banks and fintechs, see the following report: https://www.iproup.com/finanzas/7020-fintech-cuenta-machine-learning-Por-que-bancos-digitales-usan-redes-sociales-para-dar-creditos

(168) Item 29.2

(169) Item 29.3

(170) Item 29.4

(171) Item 30

(172) Item 30.2

(173) Item 30.4

(174) Item 31

(175) Item 32.2

(176) Item 32.3

(177) It should be mentioned that the regulations of both Argentina (Law 25,326, Art. 14.4) and Uruguay (Law 18,331, Art. 14) provide for it.

(178) Item 36.1

(179) Item 36.2

(180) Chapter VI

(181) Item 38.1

(182) Guide to Impact Assessments. Available at: https://www.argentina.gob.ar/noticias/argentina-y-uruguay-lanzan-la-guia-evaluacion-de-impacto-en-la-proteccion-de-datos

(183) Item 39

(184) It should be remembered that these self-regulatory mechanisms are complementary to the existing laws and therefore, form part of a co-regulation system.

(185) Item 40

(186) Item 40.2

(187) Item 40.3

(188) For example, within the document drawn up by Argentina and Uruguay, the two governments launched a guide on how to conduct impact assessments. However, as of the date of this report, this guide is not of mandatory compliance for data controllers.

(189) Item 41

(190) General Personal Data Protection Law (LGPDP) No. 13,709, Art. 38

(191) The texts that form part of the DEPA are available at https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement-depa/depa-text-and-resources/

(192) Government of Canada, "Background: Canada's possible accession to the Digital Economy Partnership Agreement" at https://www.international.gc.ca/trade-commerce/consultations/depa-apen/background-information.aspx?lang=eng

(193) See the website of Singapore's Ministry of Trade and Industry at https://www.mti.gov.sg/Improving-Trade/Digital-Economy-Agreements/The-Digital-Economy-Partnership-Agreement

(194) The Agreement, for example, mentions small and medium-sized enterprises in Art. 2.5(e) but does not provide for a detailed chapter on the subject as the DEPA in Module 10, where it even creates a "Digital Dialogue" for SMEs.

(195) DEPA, Art. 1.3; Agreement, Art. 1

(196) DEPA, Art. 4.2.1; Agreement, Art. 6.1

(197) DEPA, Art. 4.2.2 and its footnote 4.2.3; Agreement, Art. 2.5(f) and its footnote.

(198) DEPA, Art. 4.2.4; Agreement, Art. 6.3

(199) DEPA, Art. 4.2.5; Agreement, Art. 6.4

(200) DEPA, Art. 4.2.7; Agreement, Art. 6.5

(201) DEPA, Art. 4.3; Agreement, Art. 7

(202) DEPA, Art. 4.4; Agreement, Art. 8

(203) DEPA, Art. 6.3.1; Agreement, Art. 5

(204) For example, the Mercosur Resolution 037-2019 on Consumer Protection E-Commerce is available at https://normas.mercosur.int/simfiles/normativas/73867_RES_037-2019_ES_Protecci%C3%B3n%20Consumidor%20Comercio%20Electr%C3%B3nico.pdf

(205) DEPA, Art. 6.4; Agreement, Art. 9

(206) DEPA, Arts. 5.1 and 5.2; Agreement, Art. 6.6

(207) DEPA, Art. 5.1; Agreement, Art. 12(f)

(208) Agreement, Art. 6.7

(209) DEPA, Arts. 4.2.8, 4.2.9 and 4.2.10

(210) Agreement, Art. 9 and its footnote. This is consistent with Argentinian legislation.

(211) DEPA, Art. 6.2

(212) Patrícia Varejão, "The delay in closing the treaty between Mercosur and Singapore", https://www.memo.com.ar/economia/el-aplazamiento-de-la-firma-del-tratado-entre-mercosur-y-singapur/

(213) Library of Chile, Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) https://www.camara.cl/verDoc.aspx?prmTIPO=DOCUMENTOCOMUNICACIONCUENTA&prmID=79273

(214) See the Spanish text at http://www.sice.oas.org/Trade/TPP/CPTPP/Spanish/CPTPP_Text_s.pdf y http://www.sice.oas.org/Trade/TPP/Final_Texts/Spanish/Chapter14_s.pdf

(215) See Vera Thorstensen and Valentina Delich, "Convergence on e-commerce: the case of Argentina, Brazil and MERCOSUR", in Maarten Smeets, Adapting to the digital trade era: challenges and opportunities (2021), p. 246, available at https://www.wto.org/english/res_e/booksp_e/adtera_e.pdf

(216) A similar experience happened in Asian countries, where the text of the CPTPP was also quoted almost literally by other bilateral trade agreements, such as the Regional Comprehensive Economic Partnership ("RCEP") between Australia, Brunei, Cambodia, China, Indonesia, Japan, Laos, Malaysia, Myanmar, New Zealand, Philippines, Singapore, South Korea, Thailand and Vietnam. See Kati Suominen, "Two Years into CPTPP" (August 2021), at https://www.csis.org/analysis/two-years-cptpp

(210) Jane Kelsey, "DEPA Lacks Added Value," at https://www.eastasiaforum.org/2020/04/10/depa-lacks-added-value/

9. About the authors

Celia Lerman is a lawyer and partner at Lerman & Szlak, where she heads the Intellectual Property department and is responsible for the design and execution of transnational IP and privacy strategies. She is co-director of the Undergraduate Law Degree at the Torcuato Di Tella University - UTDT, and a founding member of ALAP (Latin American Privacy Association).

Gabriela Szlak is a lawyer and partner at Lerman & Szlak and a lead assistant in Digital Business, E-Commerce, Privacy and Intellectual Property focused on companies in the technology sector. She is a consultant for the World Bank and teaches Legal and Regulatory Aspects of Digital Business in Master's Degree programs at the University of Buenos Aires.

Lucia Suyai Mendiberri is a lawyer graduated from UdeSA. She specializes in Intellectual Property, Technology and Personal Data Protection. She completed the Training Program in Internet Law and Communications Technology at UdeSA and is currently doing a Master's Degree in Law and Economics at the UTDT.

adc.org.ar