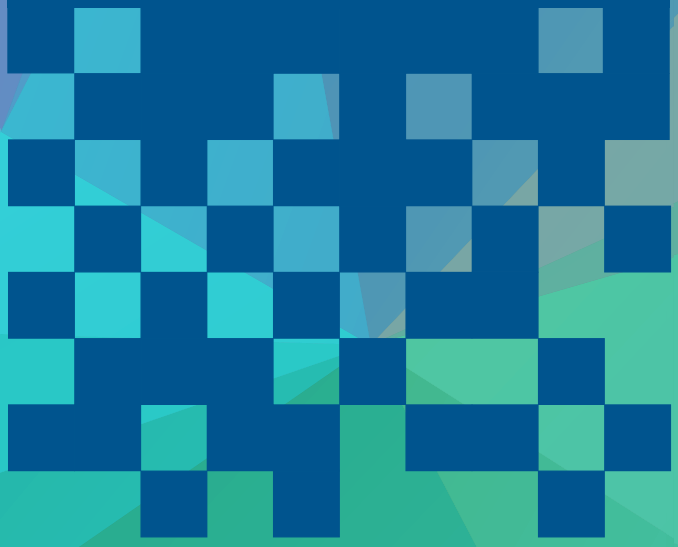
Regional digital Market

Strategic aspects



UNITED NATIONS
ECLAC

70 ECLAC
FOR SUSTAINABLE DEVELOPMENT WITH EQUALITY

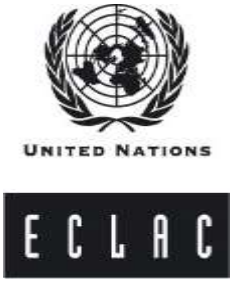
CAF DEVELOPMENT BANK OF LATIN AMERICA

german cooperation
DEUTSCHE ZUSAMMENARBEIT

Project Documents

Regional digital market

Strategic aspects



Economic Commission for Latin America and the Caribbean

This document was prepared by Jorge Alejandro Patiño and Edwin Fernando Rojas of the Production Productivity and Management Division of the Economic Commission for Latin America and the Caribbean (ECLAC), and Mauricio Agudelo of the Development Bank of Latin American (CAF). The support of Tanía García-Millán, Valeria Jordán, Wilson Peres, Laura Poveda and Sebastián Rovira of ECLAC is gratefully acknowledged.

ECLAC is also grateful for the support provided under the project "Innovations for sustainable structural change" of the programme "Structural Change for Sustainable and Inclusive Development in Latin America and the Caribbean" of ECLAC and the German Agency for International Cooperation (GIZ).

The opinions expressed in this document, which is an unofficial translation that has not undergone formal editorial review, are the exclusive responsibility of the authors and may not necessarily coincide with those of the Organization.

Publication of the United Nations
LC/TS.2018/30
Distribution: Limited
Original: Spanish

Printed at United Nations, Santiago.
S.18-00569

Contents

Tables

Figures

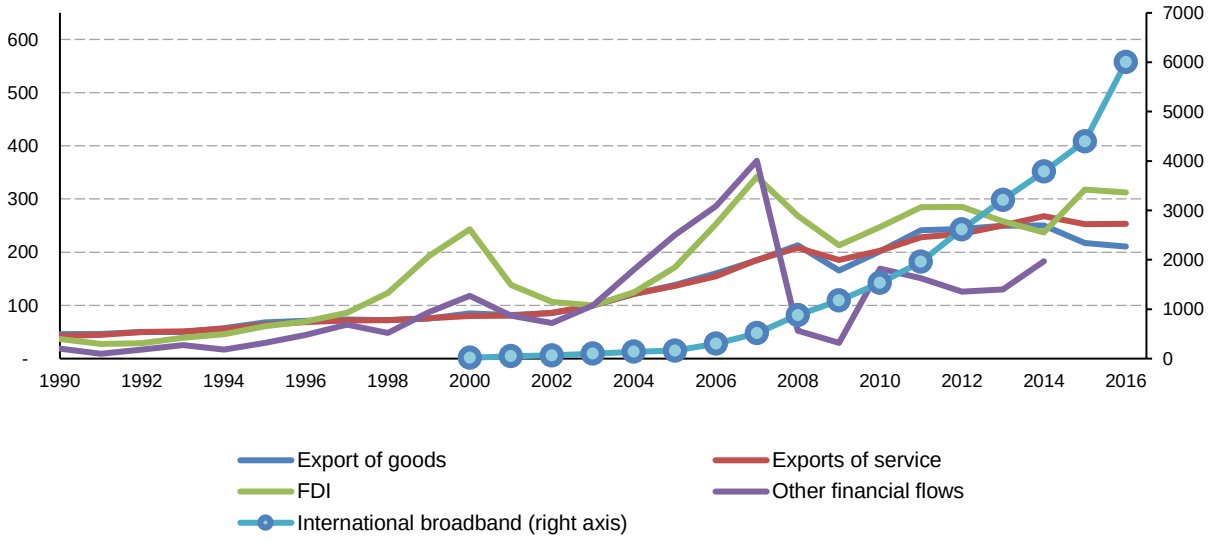
Boxes

Diagram

Introduction

In recent decades, the world economy has undergone major transformations: the liberalization of markets for traditional goods, services, and capital flows, the emergence of global digital platforms and the rapid growth of digital flows. In the last decade, the world economy has experienced an intense digital globalization in which traditional flows lost dynamism while cross-border digital flows multiplied by 45 between 2005 and 2014 (ECLAC, 2016, MGI, 2016).

Figure 1
Cross-border global flows
(Index 2003 = 100 and Tbps)



Source: ECLAC based on data from IMF, WTO, McKinsey Global Institute and TeleGeography.

Cloud computing, the Internet of Things (IoT), big data analytics, machine learning and artificial intelligence are transforming the supply and demand of goods and services, the global value chains, the

management of human and financial resources, and the capacities, functions, and productive processes. These advances not only generate new products and services, increase productivity, and incorporate billions of users, but also accentuate asymmetries between leading countries and peripheral economies, the polarization of the business world, the vulnerability of employment structures, the concentration of income, and regulatory challenges.

The United States, Western Europe, and China lead the technological revolution as evidenced by the importance of its digital infrastructure and services, innovation ecosystems, global digital platforms, and IoT advances. These countries are developing a new governance for the digital age, mainly through commercial agreements and initiatives. The United States, for example, presented 24 provisions (The Digital 2 Dozen) within the framework of the Trans-Pacific Agreement (TPP) to promote and regulate the digital economy through free and open Internet and trade without borders (USTR, 2016).[1] For its part, the European Union, in the framework of the creation of a digital single market, is developing standards for consumer protection, electronic payments, trade facilitation, and transparency (Malström, 2016). China, in addition to negotiating an extensive chapter on electronic commerce in the Regional Comprehensive Economic Partnership (RCEP), recently launched a strategy for international cooperation in cyberspace, in addition to a system of rules for privacy of cross-border data within the framework of the Asia-Pacific Economic Cooperation Forum.

In the production of goods and services, digitization takes the form of the IoT, the robotization of productive activities and the incorporation of new technologies, particularly those of large data analytics and artificial intelligence; as well as by a strong degree of substitution of traditional goods and services for their digital equivalents. New technologies have also changed the way trade is conducted, reducing the cost of providing cross-border services and connecting businesses along value chains. In particular, they help overcome many of the limitations associated with operating in international markets and lead to the adoption of new business models, the entry of competitors and a change in the sources of competitive advantages. Digitalization changes not only the way in which trade is carried out, but also who and what is negotiated; thus, a growing number of low value transactions and small shipments cross borders.

Global platforms such as Alibaba, Amazon, and eBay help the marginalized or those located in remote areas to enter markets, strengthening a pattern of more inclusive economic development.

In this new global economic context, the countries of Latin America and the Caribbean face important challenges, in particular, the development of an infrastructure for innovation and the creation of a more integrated digital market. The objective of this document is to propose elements for a strategic agenda that allows to go from a diagnosis of barriers and obstacles that prevent the expansion of the digital economy to a set of principles, objectives, and actions that guide policy decisions to advance in the formulation of a regional digital market model. In particular, the document focuses on the issues of connectivity, IoT technology, e-commerce, cybersecurity, and a description of the initiatives from sub regional associations aimed at promoting the digital economy.

[1] Although the United States withdrew from the agreement, leaving its ratification uncertain (as of the date of the publication of this document), the digital provisions could be included in an electronic commerce chapter in the renegotiation of the North American Free Trade Agreement (NAFTA).

I. Connectivity in the countries of the region

Latin America and the Caribbean countries continue to progress in the use and access to telecommunications services. Through different connection modalities, 56.4% of the region's population used the Internet in 2016, close to 9 percentage points (p.p) higher than the world average. However, when compared to OECD countries, the European Union (EU) or North America (Canada and the US), the gap is greater (20 p.p.).

Table 1
Penetration of Internet and user gaps by regions and groups of countries, 2013-2016

	Percentage of Internet users			
	2013	2014	2015	2016
LAC	46.2	48.7	54.2	56.4
OECD	75.6	77.3	78.8	80.9
Emerging countries	34.1	37.8	41.4	44.6
EU27	75.6	77.2	78.5	80.8
North America	72.8	74.4	75.9	77.5
Asia and the Pacific	30.7	34.6	38.2	41.9
World	37.2	40.5	43.8	47.1
	Gaps (percentage points)			
	2013	2014	2015	2016
LAC-OECD	-294	-28.5	-24.6	-24.5
LAC-Emerging countries	12,1	10.9	12.8	11.8
LAC-EU27	-29.4	-28.5	-24.3	-24.4
LAC-North America	-26.6	-25.7	-21.7	-21.2
LAC-Asia and the Pacific	15.5	14.2	16.1	14.5
LAC-World	9.1	8.2	10.4	9.2

Source: ECLAC (2017) based on ITU data.

The main modality of Internet connection in recent years has been mobile broadband (MB). By 2011, subscriptions to this service have already doubled to fixed subscriptions and, since then, its average annual growth rate has been 36.4%, while fixed broadband stood at 8.9%. In 2016, active subscriptions as a

percentage of the population for fixed and mobile connections were 11.2% and 64.3% respectively. Despite the strong growth of the MB, there is still a significant gap with OECD countries (35 p.p.), while for fixed broadband, the gap has remained close to 20 p.p.

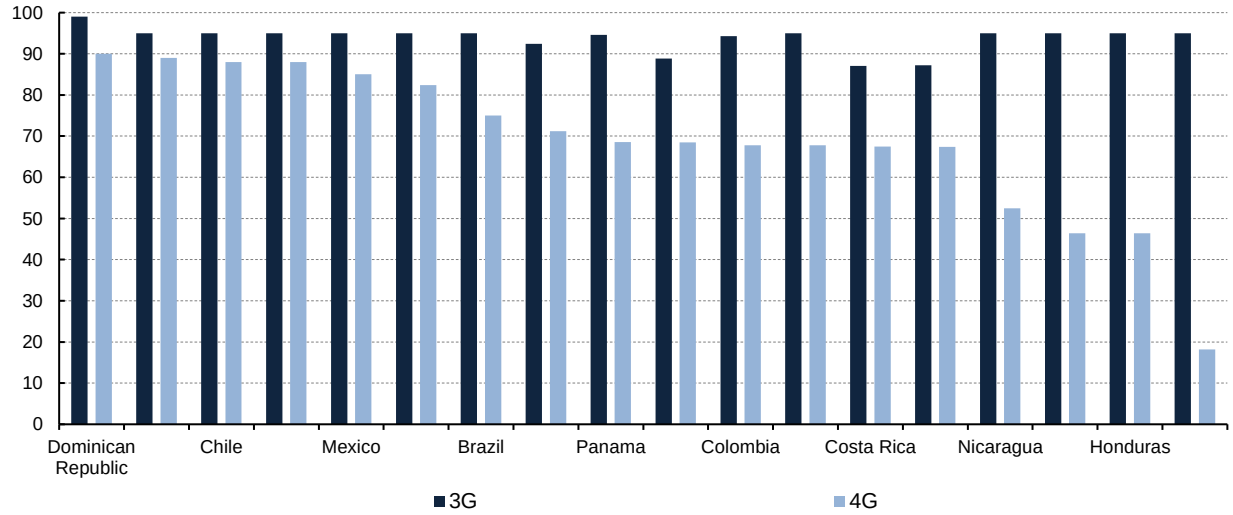
Table 2
Penetration of fixed broadband and user gaps by regions and groups of countries, 2013-2016

Percentages of people with fixed broadband				
	2013	2014	2015	2016
LAC	9.2	9.8	10.6	11.2
OECD	29.5	30.2	31.3	32.1
Emerging countries	7.7	8.1	10.7	12.2
EU27	29.9	31.0	32.1	32.9
North America	30.4	30.8	31.9	32.9
Asia and the Pacific	7.8	7.9	8.9	10.5
World	9.9	10.1	11.2	11.9
Gaps (percentage points)				
	2013	2014	2015	2016
LAC-OECD	-20.3	-20.4	-20.7	-20.9
LAC-Emerging countries	1.5	1.7	-0.1	-1.0
LAC-EU27	-20.7	-21.1	-21.5	-21.7
LAC-North America	-21.2	-21.0	-21.3	-21.7
LAC-Asia and the Pacific	1.3	1.9	1.6	0.7
LAC-World	-0.7	-0.3	-0.6	-0.7
Percentage of people with mobile broadband				
	2013	2014	2015	2016
LAC	33.3	49.4	59.3	64.3
OECD	78.9	85.9	94.2	99.8
Emerging countries	17.8	28.9	38.1	46.4
EU27	60.1	69.3	75.8	82.1
North America	93.2	97.9	110.1	114.7
Asia and the Pacific	18.5	29.4	37.7	42.6
World	27.3	36.7	44.2	49.4
Gaps (percentage points)				
	2013	2014	2015	2016
LAC-OECD	-45.6	-36.5	-34.9	-35.5
LAC-Emerging countries	15.5	20.6	21.3	17.8
LAC-EU27	-26.8	-19.8	-16.5	-17.8
LAC-North America	-60.0	-48.5	-50.8	-50.4
LAC-Asia and the Pacific	14.8	20.0	21.7	21.6
LAC-World	6.0	12.7	15.1	14.9

Source: ECLAC (2017) based on ITU data.

The deployment of mobile broadband was accompanied by technological advances to improve service quality. In the first quarter of 2017, most countries of the region had between 90 and 100 percent of their population covered by 3G networks. In the coverage of 4G networks, there is still much heterogeneity between countries: in many it is almost equal to 3G coverage, in others it reaches close to 60% of the population, and in some it is less than 20%.

Figure 2
Coverage of 3G and 4G networks, first quarter of 2017



Source: ECLAC based on GSMA (2017).

Despite progress, the region still lags strongly compared to the developed world; therefore, efforts to reduce or even eliminate those gaps should be increased. In addition, countries should de promoting the incorporation of advanced technologies in productive sectors, in which new gaps deteriorate the productivity and the competitiveness of the region.

II. Infrastructure for the Internet of Things[2]

The IoT is based on cyber-physical systems supported by big data analytics and cloud-computing. Cloud solutions, high processing and transmission speeds, and large data analytics have facilitated the collection, storage, and processing of large amounts of information. This has been supported by the reduction in costs of devices and transmission networks. The IoT exceeds the initial concepts of machine to machine (M2M) directed at specific interactions in closed systems. The massive collection of data by IoT devices can be used in complex processes in real time and affect not only things but also people.

On its own and in conjunction with other advances, IoT is part of the migration towards a more sophisticated production economy based on open and interactive structures. The enabling infrastructure not only consist of connectivity (fixed, mobile, and satellite) but also of the infrastructure that allows the processing, storage, and processing of information, and the analysis of large data, as well as by applications that allow automation, facilitating its use in activities that favor innovative products and services. Access technologies that can support IoT include:

Fixed access. It is mainly developed through the HFC (Hybrid Fiber Cable) networks used for subscriber TV and fiber optic networks. Both can be used for the IoT, and in addition, the operators of these networks also target the development of wireless and mobile services. In this case, the objects are connected to a gateway that uses the IP link for its routing in both directions towards the core of the application.

Wireless access. LPWAN and other 3GPP access technologies. They are linked with mobile technologies; therefore, they inherit their security and privacy advantages from mobile networks, as well as the confidentiality of the user's identity, authentication, data integrity and the identification of the devices, except when the data goes beyond their scope.

Wireless access. Proprietary LPWAN access technologies. There are many proprietary technologies that operate mainly in an unlicensed spectrum. In addition, others used established standards such as WiFi or Bluetooth. In general, the characteristics of a Low-Power Wide-Area Network (LPWAN) are:

- Low power: are designed for a battery life of up to 10 years or more, depending on the intensity of use.
- Long reach of access: up to 10 km from the gateway from which they enter the network.

[2] This section is based on Omar, D. (2017), "Apoyo a la implementación del Programa Estratégico de Especialización de Industrias Inteligentes", document prepared for the project Collaboration Agreement ECLAC and CORFO, Santiago de Chile, unpublished.

- Low data speeds: generally, less than 5 Kbps.
- Data volumes from 20 to 256 bytes per message and a few times per day.
- Most of them have star topology.
- They can operate with 140-160 db of trajectory loss, coverage, or Maximum Coupling Loss (MCL).
- Receiver sensitivities of more than -130 dbm, which are the main determinants of high coverage values.[3]

There are many LPWAN technologies, including those of the 3GPP[4] LTE-Cat M1 and NB-IoT group. LPWAN is also used as a backup for cellular networks for alarms (required by regulation in some countries). It is useful for the interiors of buildings, for example, basements, where the measurers are usually located. Also, coverage could be deploy with LPWA networks instead of cell phones.

While 3GPP access technologies were being developed for IoT, proprietary technologies emerged such as Long Range Wide Area Network (LoRa), Random Phase Multiple Access (RPMA), and Sigfox.

Subsequently, work continued with other access technologies with similar characteristics and topologies include, for example, retransmissions in user units.

Sigfox and LoRa appeared about 18 months earlier than similar 3GPP technologies, which gave them time to deploy and be used in the initial demand for IoT connectivity. These technologies allowed operators to enter the market, relying on the subsequent convergence of both types of access technologies. By gaining market share, these technologies expected to compete with 3GPP. These suppliers are complementary and not compete with operators, although the position of the operators varies according to the country.

Integrated SIM cards. Provide an important degree of security and store data to authenticate its users. Among these identifiers, are those for the identification of the network; the International Circuit Card Identifier (ICC-ID); the International Mobile Subscriber Identity (IMSI) through which the SIM communicates with the mobile network; and the Ki key for the authentication of the card in the mobile network, and the identification of the local area in which the user is located, which changes the local network change.

Although for the terminals the possibility of changing the SIM card from one computer to another is desirable and simple, the situation for IoT devices is more complicated or even impossible: thousands of devices need to be modified, located in remote places or are difficult to reach, or in welded cards, used for safety reasons and damage prevention.

For this reasons, the embedded SIM technology from GSMA has been developed, which allows, through a procedure contained in agreed specifications, that SIMs can be distributed globally for IoT. Also, they allow the change of provider without physical access to the terminal. This technology has enabled the massive use of mobile terminals for IoT, reducing costs by simplifying the procedures for changing the provider and facilitating the integration of the SIM to the device with its tests.

These specifications are fulfilled in the embedded Universal Integrated Circuit Card (eUICC) that is produced as a microchip or as common cards. A noteworthy aspect for IoT is that eUICCs support multiple SIM profiles and, therefore, multiple sets of credentials, which allows the entry to different operators, albeit one at a time. In this way, terminal equipment can have a main operator and a secondary operator.

According to the policy defined for the service, it is possible to switch to the secondary operator in case of failure of the principal one. You can also count on several operators in an eUICC to further facilitate switching between operators. The eUICC allows the IoT provider to remotely change the provider of connectivity over the life of the service it provides without incurring additional costs involved in accessing each terminal equipment to change it.

An additional step that is required for the IoT, inevitable in critical applications, is that it is possible for multihoming —maintain permanent connection with more than one network simultaneously— and load balancing.

[3] Shannon's theorem through low transmission speeds, allow these levels of sensitivity in the receivers.
[4] 3rd Generation Partnership Project.

Spectrum

Progress in the IoT will lead to an increasing use of the spectrum, although it is not possible to know in advance what type of use will be applied to each band. The case of unlicensed bands is even more unpredictable due to the conjunction of multiple "non-disciplined" technologies, that is, not subject to the conditions that exist in the licensed bands. These issues are key in updating the regulation of spectrum use considering that thousands or hundreds of thousands of IoT terminals will have lifetimes of 10 or more years. It is necessary to anticipate the use of spectrum for technologies that are not fully defined, for an estimated use, with the need of providing regulatory stability to suppliers for 10 or 20 years. A typical case to analyze is the use of 2G networks, which are being replaced by more advanced technologies, according to the evolutionary process of the mobile service. The definitive exit of this service could be blocked by the new 3GPP EC-GSM-IoT standard that is mounted on these 2G networks.

In principle, there are no impediments for IoT applications to operate on a licensed or unlicensed spectrum, this depends on the application that it is going to be supported. In critical applications, such as medical or aeronautical, achieving maximum security in connectivity means that a licensed spectrum needs to be use, apart from other measures. In other cases, for example, agricultural applications, intended for the collection of information, would not be affected by interference in unlicensed spectrum. These applications have repetition protocols that, taking advantage of the fact that there are no critical deadlines, ensure the fidelity of the information.

In general, the entire spectrum suitable for IoT (not very high frequencies) is occupied by other services, encumbering the choice of which spectrum to use. Regulators seek to release bands for these and other uses paying attention to allocation efficiency. Users who face uncompetitive connectivity offers from licensed service providers seek regulatory arbitrage and use unlicensed bands. These have an additional advantage for service providers as they can modify access technology with fewer restrictions than when using a licensed band. They reduce the costs of introducing a modification. They are a good spectrum solutions for deployments of technologies from scratch or greenfield, favoring innovation and start-ups.

Among unlicensed bands, the most saturated is of 2.4 GHz because, although it originally was universally designed for industrial, scientific and medical applications, it was progressively being used for other applications; also, it is one of the most used by WiFi and Bluetooth. A strong increase in the use of the 900 MHz band is also expected in Region 2 —which mainly includes the Americas and the Caribbean— since it allows good coverage and saves energy. For this reason, there are studies, for example, from the European Conference of Postal and Telecommunications Administrations (CEPT)[5], that explore technologies that improve the coexistence of different solutions for an efficient use of a shared spectrum for IoT, and the mitigation of harmful interferences.

In the area of access technologies in a licensed spectrum, the requirements of mobile user equipment for voice and data imply high power consumption due to the fact that the service is being improved. This is not a problem for the current mobile terminals, but it is a problem if there is a need to use similar terminals for IoT; therefore, 3GPP terminals have been developed aimed at lowering energy consumption.

Additionally, concept tests are currently being carried out for several technologies that aim at reducing battery consumption and the use of more expensive networks. An example is a connectivity project in the United Kingdom for smart meters that use a combination of cellular access infrastructure and an IPv6-based access grid, using other measurers as intermediate nodes with the 802.15.4[6] protocol. In this case, the contracts are made for 15 years, which shows that access technologies and business models are being established.

When an IoT application is developed, the choice of the band spectrum, licensed or not, determines the size of the devices. Although it occurs that a higher the frequency, the smaller the size, at higher frequency there is less coverage and penetration in buildings.

[5] http://www.cept.org/.

[6] IEEE 802.15.4 is a physical level protocol and medium access control (MAC) for wireless personal area access networks (PAN) that use low data rates.

With regards to the allocation of bands for IoT, situations between countries varies. In general, there is no preferred bands, although there is awareness that the spectrum must be analyzed carefully because it is critical for the development of IoT. CEPT indicated in a 2015 report that in Europe there was not a strong case to justify the allocation of exclusive bands for IoT. But by mid-2016, the feasibility of enabling a spectrum in the 700 MHz was being considered, and by the end of 2016, the Radio Spectrum Policy Group (RSPG), through a spectrum roadmap for IoT, began to analyze this topic in depth.

For its part, the Office of Communications (OFCOM) of the United Kingdom has allocated bands of unlicensed use for IoT applications. In September 2015, after a consultation process, it concluded that there was no need for a new license to deploy services in the 55-68 MHz, 70.5-71.5 MHz and 80-81.5 MHz bands, and that the current licenses in these bands were able to provide IoT and M2M services.

Finally, 5G networks will have more capacity than current networks and will be prepared as IoT access networks. Nevertheless, the problem of reach will persist, which depends on the band of use. These networks will surely collect multiple current requirements, especially for IoT, such as low latency or adequate availability for critical applications.

It is necessary to add to the physical infrastructure activated for IoT, essential aspects such as a balanced model of privacy and cybersecurity systems. This is important to avoid information leaks and support the acceptance of this new technology among potential users.

The harmonization of the spectrum at the broadest geographical level is necessary to reduce the costs of terminals and operations (economies of scale). Therefore, among the relevant aspects to promote IoT in a context of a regional digital market include:

Standards and interoperability, regional and global harmonization. Standards are important for the creation of markets for new technologies. In the IoT, there are several service layers. The compatibility between similar layers of different manufacturers or operators must be ensured, as well as the vertical compatibility to avoid dominant positions and the impediment of development. The problem of incompatibility is clear when using proprietary technologies, even when using centralized or decentralized topologies; but it could be resolved with gateways at the level of the data aggregation layer. There may also be incompatibilities in the layers of initial data processing, pre-selection of data, storage, integration, processing or activation of devices. It is enough to observe the inconveniences of a user who wants to change his equipment maintaining the same service. For example, one may lose data or see that some applications are no longer operable.

Thus, it is important to work on the promotion of standards and interoperability in the aforementioned aspects, in addition to data formats, security mechanisms and privacy protection, which must also be evaluated with standardization and interoperability goals, if possible, at the larger geographic scale (regional and global).

Transition to IPv6 and numbering systems. The IPv6 protocol has many advantages over IPv4 for the deployment of IoT. In particular, it allows to have enough IP addresses for terminal devices connected to the Internet, without the need to share IPv4 addresses, as is the case in many countries with so short deployment of IPv6 access points. Government institutions can be drivers for migration to IPv6. In the transition period, it should be analyzed if there are no numerical obstacles for the expansion of the number of IoT equipment or roaming costs that hinder cross-border services.

Government development policy for IoT. Governments have a powerful role in promoting the deployment of new technologies: their institutions can deploy their services supported by these technologies. These actions, generally initiated through competitive processes, encourage current and potential operators to be prepare to offer their services for specific uses and include the deployment of IoT in their plans before moving to validation phases, proofs of concept and other stages prior to commercialization. In addition, the opportunity to obtain a contract with the government, is an incentive for operators as proof of experience.

It is desirable, in these cases, the selection of government services with strong impact on the promotion of technology, seeking a balance between cost and benefit. It is also important to boost markets and fine-tune business models.

These deployments, if they come early, allow to observe, analyze, and take corresponding actions related to workforce capabilities and the degree of preparation to operate IoT; for example, begin its incorporation in the health sector by monitoring non-critical patients.

Policies and regulations on privacy, protection, and use of data. Privacy policies must develop a regulation for the use of data from the IoT that respects privacy and allows it's use. Thus, attention is paid to the use of sensitive data for users through clear and public guidelines that include their consent; this would make it possible to avoid restrictions on the development of the IoT and the analysis of big data.

Serious cases of information leakage can damage trust in these systems and delay and restrict their development. It is clear that the apps collect a lot of personal information without major limitations. But, in the IoT there will be an even greater amount of information with greater detail, and surely with fewer warnings or notices compared with apps. Small devices do not allow a reliable interaction with users to ask specific permissions, as it happens on the screens of mobile devices. In the field of industrial applications, the complete system is under a more centralized and stricter control than in applications for individual users. In these cases, the user can limit the type of information that is been shared.

Notwithstanding, from another point of view, limitations in the type and quantity of information would make the IoT lose a positive externality related to the possibility of adopting policies guided by analytics: processes that improve, for example, traffic management by analyzing trends and profiles based on big data.

The latter issue is important in the definition of policies and regulations, mainly for making anonymous the data as soon as possible from the user's computer, or from the first point of concentration of information. From the technical point of view there are difficulties, due to the low processing capacity of these equipment's, to make data anonymous from the initial phase of entry into the system.

In some countries, regulations about localization prevent the provision of cross-border services using centralized servers, particularly on hosting national data abroad. Additionally, IoT devices can collect information in one jurisdiction and process, store, analyze, and use it in other. This depends on the operation of the applications that requires it and from the search for efficiency and the improvement of the quality of services by centralizing information.

Security policies. The IoT, due to its massive deployment and the low cost of terminals, it is at high risk for attacks. This makes the use of sophisticated security systems through encryption impossible. Criminal activities can attack devices (as happened with camera codes in 2016), access links and even servers, often housed in the cloud. In all cases, they would access a valuable mass of information or important controls. They can take control the system and even attack a factory or a public utility directly, leaving them inoperative, distort the functioning of a health care system or cause accidents with connected cars.

Although it is impossible to have a solution that avoids any attack, risks can be reduced by carefully designing the safety of the equipment, circulating access and transporting to networks only essential information. Several levels of security should be established in the core of the network, reinforcing access controls to the devices, and mainly designing equipment that accepts software updates that eliminate vulnerabilities. This is particularly important considering that these devices can be operating during very long periods and in places of difficult access.

Failures in security burden the development of the IoT. Security is in the hands of operators of access networks and data centers and the regulation of the resilience of the IoT networks is fundamental to generate user confidence.

Management of the radio spectrum. The spectrum is the basis of access networks, in this sense, the authorities should consider the allocation of the largest possible spectrum for mobile services for two reasons:

- The increase directly impacts the reduction in the cost of access infrastructure. The more spectrum is available in a radio base, the more traffic it can support and, therefore, the lesser need to install additional base stations for traffic reasons.

- An available and unassigned spectrum, when there are no present or future impediments, is a recurring loss of value by society.

Considering the uncertainty regarding the spectrum, as well as the difficulties to make initial estimates of its use in the future, it is convenient to develop a light touch policy regarding the allocation of bands, liberalizing its use as soon as possible to facilitate the deployment of networks. That is, observe the present requirements and their trends in the spectrum bands currently been used (licensed and unlicensed), observe what other bands can be allocated for these IoT accesses and determine according to those requirements the actions to be followed.

The growth potential for the IoT is large and consists of different types of access capacity requirements ranging from sensors with very low data traffic to devices that require high definition images and very low latency (medical activities), passing through industrial devices with higher bandwidth consumption. While it can be discussed what technologies will be used in each case, the issue is not fully defined, as seen in the uses being developed by large operators combining a licensed spectrum and 3GPP technologies, with an unlicensed spectrum and proprietary technologies. It is unknown where the greatest consumption of capacity and spectrum will occur, and whether it will occur in a licensed or unlicensed spectrum.

Despite this, an increase in spectrum use can be expected in different bands and under licensed, unlicensed regimes, and a combination of both. This would be a continuation of the current situation. There could also be formal situations of assignment of licensed a hybrid spectrum, but with authorization to extend the service to the unlicensed spectrum under certain conditions. It may be necessary to attribute bands of spectrum for common use with the imposition of technical and administrative conditions, but subject to the fact that it does not produce interference or request protection from other authorized telecommunications services of a different category.

Given that regulatory frameworks should encourage efficiency in the use of the spectrum, the analysis of trends in IoT is necessary in order to not allocate and assign unnecessary spectrum.

In relation to the licensed spectrum, in particular where voice services are predominant and to a lesser extent those of data - considering the high percentage of data traffic diversion to WiFi, approximately 50% in Europe and the United States - it is necessary to consider the following points:

• If there is a significant increase in the use of the spectrum, new bands can be licensed.

• Additionally, and of high importance, technologies such as LTE-Unlicensed (LTE-U), Licensed Assisted Access (LAA) and Enhanced Licensed Assisted Access (eLAA) have been developed. LAA / eLAA allows operators to derive part of the traffic from the licensed bands to those not licensed, in particular to the 5GHz.

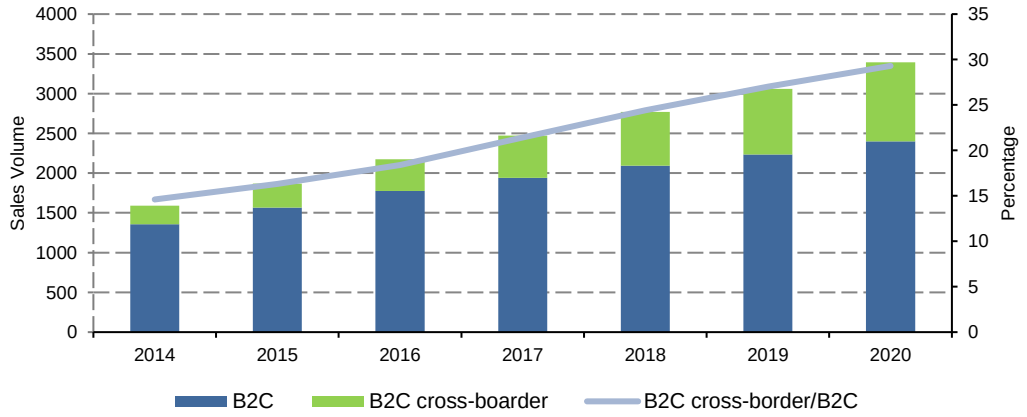
• Other technologies such as WiFi First allow the derivation of voice and data communications over WiFi networks when hot spots are available.

At the moment, it does not seem necessary to have a licensed spectrum defined for IoT, since the relationship between demand for IoT and spectrum is in an evolutionary process. It is important to observe whether, under licensing conditions, there are undesirable impediments to the deployment of IoT access technologies. More specifically, considering the direction that 3GPP has taken to generate three standards for IoT oriented at sharing the spectrum currently used by 2G/3G/4G networks.

III. Regional electronic commerce

Statistics on cross-border e-commerce are scarce and face a series of methodological challenges for their collection.[7] However, recent estimates suggest that cross-border e-commerce between companies and individuals (B2C) will reach approximately U$1 trillion per year by 2020, accounting for 30% of retail e-commerce (AliResearch, 2014). While caution should be taken with regards to these estimates, especially given the strategy of multinational companies to create online stores nationwide[8], it is important to recognize the growing weight of digital commerce of digitized products that can be downloaded or transmitted over the Internet (audio, video, printing, games, and software). For example, in 2011, more than 40% of the worldwide revenue from video games came from digital sales; in music, the figure reaches almost a third (UNCTAD, 2015).

Figure 3
B2C cross-border e-commerce, 2014-2020
(Billions of dollars and percentages)



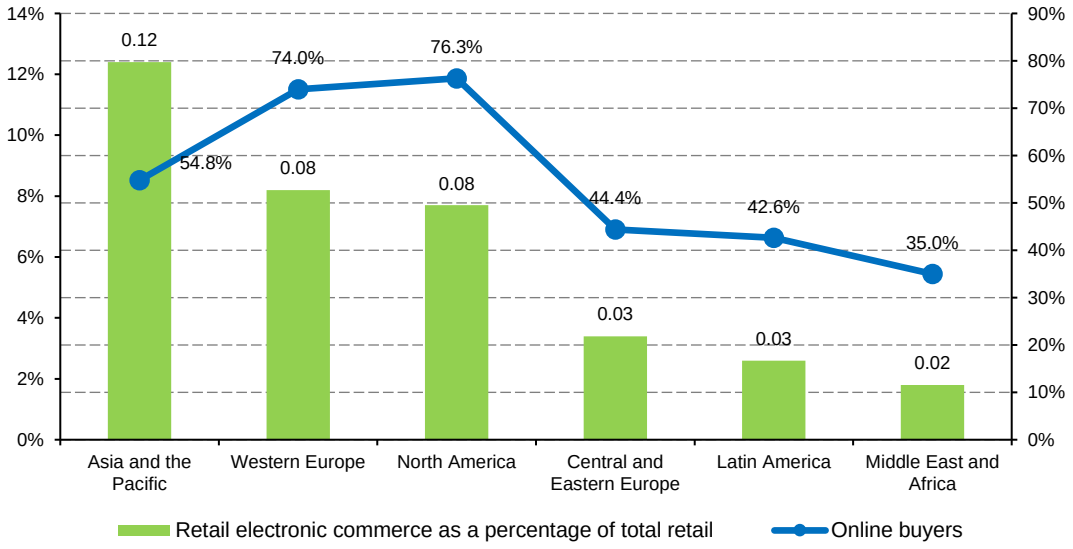
Source: AliResearch (2014), Global Cross Border B2C Ecommerce Market 2020.

[7] This section is based on the OECD & WTO document (2017), "Aid for Trade at a Glance 2017: Promoting Trade, Inclusiveness and Connectivity for Sustainable Development", OECD Publishing, Geneva.

[8] Sales that would not be considered cross-border e-commerce.

A significant number of companies carry out online business transactions in Latin America and the Caribbean. On average, 82% of companies in the region said they use the Internet to interact with their clients (UNCTAD, 2017). Also, the private estimates show that the market of retail electronic commerce will have a sustained growth in the region in the coming years, projecting sales close to U$50 billion for 2016, with a compound annual growth rate of 19%. Argentina, Brazil, and Mexico are the main e-commerce markets in the region, representing about 73% of the sales. Consequently, the growth potential is significant; in the region, this segment is equivalent to 3% of total retail trade, while it reaches 8% and 12% in North America, and Asia and the Pacific, respectively (eMarketer, 2015).

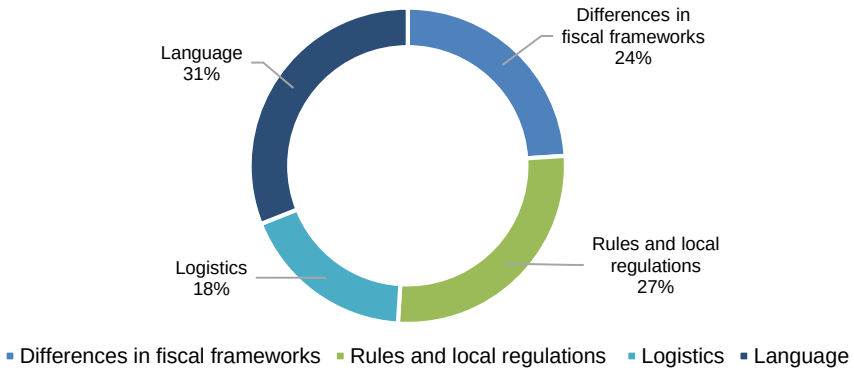
Figure 4
E-commerce as a percentage of retail and online buyers penetration, by region, 2016



Source: eMarketer (2015), Worldwide Retail Ecommerce Sales.

The growth of cross-border electronic commerce faces issues that are blocking its further expansion. In a recent survey of merchants, commercial service providers, payment service providers and consultants, the fiscal, regulatory, logistical, and language issues were identified as the main barriers to the development of cross-border electronic commerce. The need to comply with different tax and legal frameworks can be a disincentive for companies to expand their online commerce services. Likewise, the different consumer rights laws that govern the procedures for resolving complaints and returns of items differ from country to country. Regulations on privacy and data protection can hinder interregional data exchange. On the other hand, the different tax fees and tariffs to which some of the goods and services are subject on the Internet may affect the levels of competition. Finally, although language differences can be a barrier to online commerce, this aspect can be a competitive advantage for companies in the region (Keira McDermott, 2015).

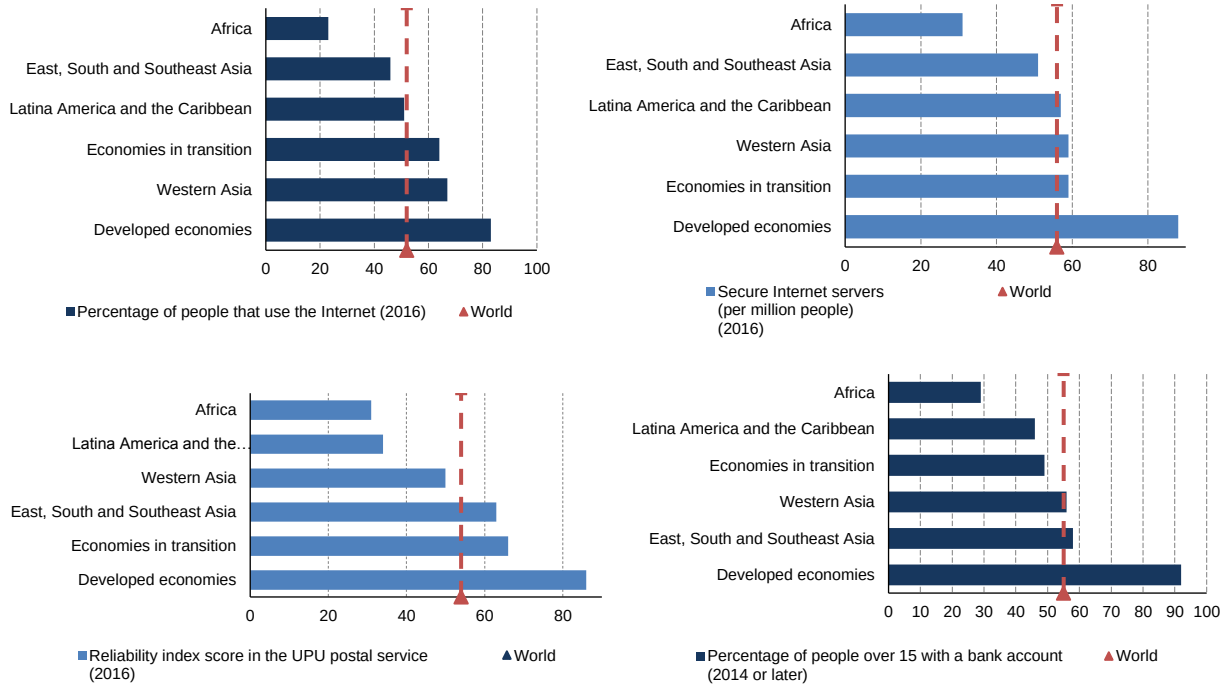
Figure 5
Main barriers to cross-border e-commerce worldwide
(Percentage of respondents)



Source: Keira McDermott, Payvision (2015), Key Business Drivers and Opportunities in Cross-Border Ecommerce.

Although the reasons vary between countries, the factors that hinder the deployment of electronic commerce are related mainly to matters dealing with access to technology and networks, cost factors, uncertainty of payment methods, legal frameworks, poor distribution logistics, and the return of products. The electronic commerce index of the United Nations Conference on Trade and Development in its 2017 version shows that, in Latin America and the Caribbean, all the indicators are below the world average. The main barriers would be the low use of credit cards and poor postal reliability (UNCTAD, 2017a).

Figure 6
E-commerce index (B2C), by regions, 2017



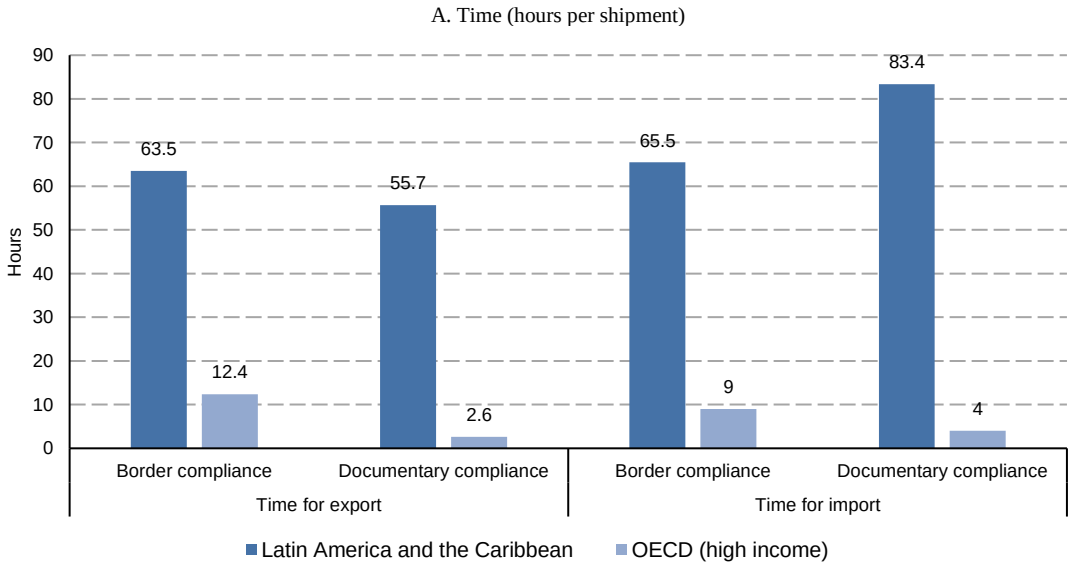
Source: ECLAC based on UNCTAD (2016), B2C eCommerce Index.

A. Cross-border paperless trade

The reduction of non-tariff costs is essential to promote regional trade, including electronic commerce. The costs of intra-regional trade in Latin America and the Caribbean are greater than those of the region's trade with the United States[9]. Likewise, the region is falling behind compared to more developed countries regarding the average cost and time to the export and import goods. These barriers are the result of infrastructure and administrative inefficiencies. Facilitating these trade mechanisms is important for several reasons, including the promotion of the internationalization of companies —in particular SMEs— and in overcoming the lack of productive diversification and integration into global value chains. It is estimated that by implementing some measures to facilitate intraregional trade, it could increase by 19% (ECLAC, 2015).

Trade facilitation requires the consideration of matters such as the improvement of institutional arrangements to favour cooperation among government agencies, increased transparency in information related to new regulations and tariff classifications, and the application of procedures that improve paperwork.[10] A central aspect of these types of measure refers to trade that takes place based on electronic communications, including the exchange of data related to trade and documents in electronic formats, better known as paperless trade.

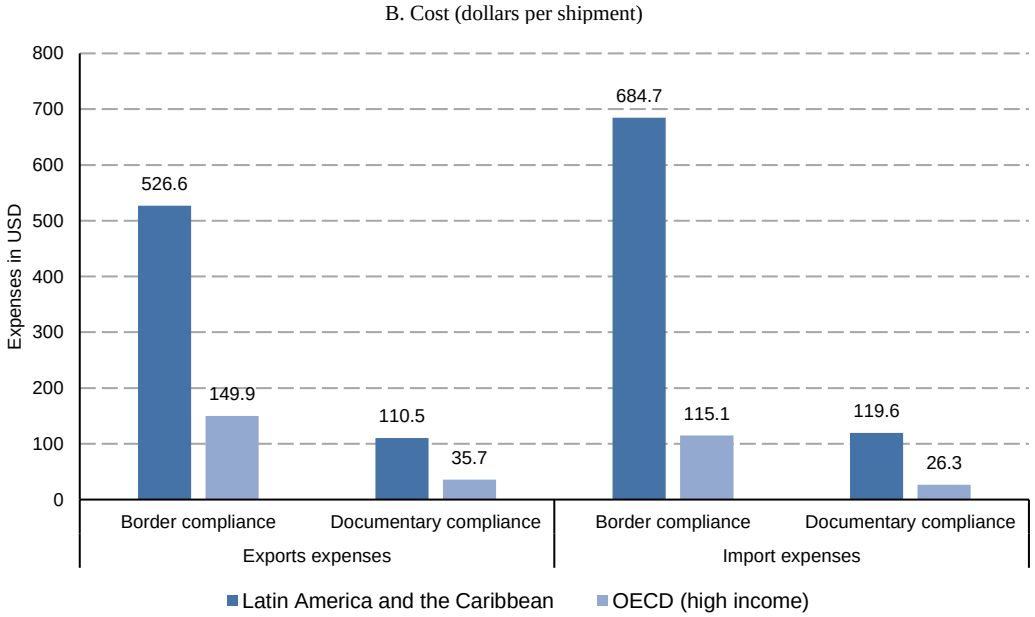
Figure 7
Latin America and the Caribbean and the OECD (high-income members)
Average time and cost of exports, 2016



[9] Trade between Central America and Mexico, and South America can reach a non-tariff tariff cost of about 124%, while the cost of trade between Central America and Mexico with the United States reaches an equivalent of 66%.

[10] Several of these issues have been discussed in the World Trade Organization through the Trade Facilitation Agreement (TFA), which contains provisions to expedite the movement, release and clearance of goods, including goods in transit. The TFA entered into force on 22 February 2017, after the ratification of two thirds of the WTO members.

Figure 7 (concluded)



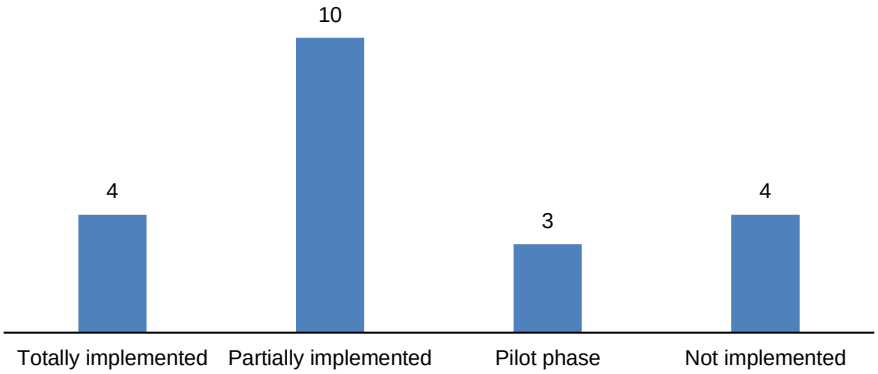
Source: ECLAC (2017) based on the World Bank, Doing Business.

The Global Study on the Facilitation of Trade and Paperless Trade (United Nations Regional Commissions, 2017), is a project that aims to monitor the implementation of global trade facilitation measures and identify good practices and training needs and/or technical and financial assistance. This analysis is based on a survey reviewing 45 measures grouped into nine categories: i) transparency; ii) formalities; iii) institutional arrangements; iv) paperless commerce; v) cross-border paperless trade; iv) cooperation among border agencies; vii) transit facilitation; viii) trade facilitation and SMEs; and ix) trade facilitation and women.

Among the measures reviewed in relation to paperless trade these include: i) electronic request for the reimbursement of customs payments; ii) electronic payment of tariffs and fees; iii) request and electronic issuance of certificates of origin; iv) electronic sending of air cargo statements; v) electronic application and issuance of licenses and permits; vi) electronic sending of customs declarations; vii) cross-border Internet connection; viii) electronic/automated customs system; ix) electronic single window for foreign trade (ESW); and x) electronic customs reimbursements. A sample of 21 countries in Latin America and the Caribbean shows an average rate of 72% of compliance with these indicators. The indicators with the lowest level of implementation are the application and electronic issuance of certificates of origin (62%), the electronic single window (56%), and the electronic request for the refund of customs payments (29%). The use of the electronic single window is most successful factor in paperless trade. This window eases the parties involved in trade and transport of goods to present documentation and other requirements in one single place (United Nations Regional Commissions, 2017).

As part of the implementation of cross border paperless trade, are the bilateral or multilateral cooperation measures that refer to: i) the establishment of laws and regulations on electronic transactions; ii) the recognition of an authentication authority for digital trade certificates; iii) cross-border exchange of trade-related data; iv) electronic exchange of certificates of origin; and v) electronic exchange of sanitary and phytosanitary certificates. The most important step in this area is the adoption of laws and regulations for electronic transactions, with an implementation rate of 76% in 21 countries. This measure is followed by the recognition of the authentication authorities of digital certificates to ease traders to conduct electronic transactions (48% of application), and the cross-border exchange of data related to trade (52%). The measures least adopted refer to the electronic exchange of certificates of origin (38%) and the electronic exchange of sanitary and phytosanitary certificates (19%).

Figure 8
Number of countries in Latin America and the Caribbean in the different phases of implementation of the Electronic Single Window (ESW), 2017



Source: ECLAC (2017), based on the Global Survey on Trade Facilitation and the Application of Electronic Commerce.

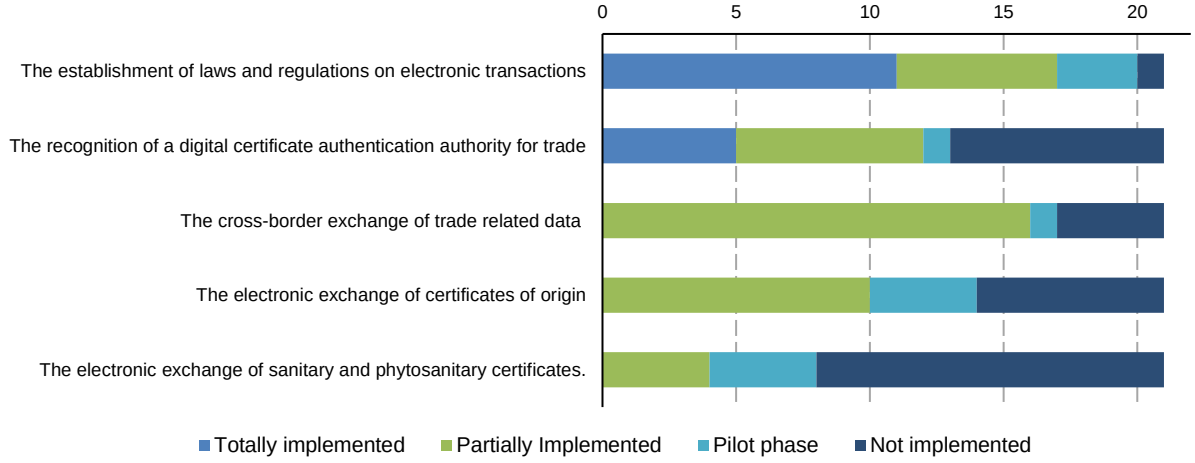
The central measures to facilitate the exchange of electronic data and documents related to trade are the existence of laws and regulations for electronic transactions and the recognition of an authority to issue digital trade certificates. However, the latest review on the implementation of these actions indicates that only 11 of 21 countries in the region have implemented laws and regulations on electronic transactions: 6 countries have partially implemented these types of standards; 3 countries are in a pilot phase; and one country does not have any laws and regulations in this area. On a lesser frequent situation is the recognition of authorities for the authentication of digital certificates, so traders can conduct electronic transactions. The adoption of this measure is very limited: only 5 countries implemented it, 8 countries did not implement, 7 countries show partial compliance, and one country is in a pilot phase.

One of the main efforts at regional level for the electronic issuance of certificates of origin is the Digital Certificate of Origin Project of the Latin American Integration Association (ALADI), which includes Argentina, Bolivia, Brazil, Cuba, Chile, Colombia, Ecuador, Mexico, Panama, Paraguay, Peru, Uruguay, and Venezuela. This project has achieved important developments in the management of certificates of origin in digital format for cross-border trade, for which it has developed an infrastructure of public keys. Up to now, entities that issue and receive digital certificates have been authorized in 8 countries. The project hopes to extend its implementation at regional level (ALADI, 2013).

Likewise, in the Common Market of the South (MERCOSUR), agreements have also been signed that allowed the recognition of advanced electronic signatures and the adoption of electronic means in customs operations in Argentina, Brazil, Paraguay, Uruguay, Venezuela, and Bolivia. These agreements are established in Resolution No. 37/06 on the recognition of the legal effectiveness of the electronic document, the electronic signature and the advanced electronic signature within the scope of MERCOSUR and Resolution No. 34/06 for the conclusion of mutual recognition agreements of advanced electronic signatures in the field of MERCOSUR. Likewise, in the Andean Community, Decision 571 on the customs value of imported goods has boosted the use of digital signatures in electronic declarations in customs offices in Bolivia, Colombia, Ecuador, and Peru. Within the framework of the Council of Ministers of Central American Economic Integration, the efforts made by Guatemala, Honduras, Nicaragua, Panama, and the Dominican Republic with respect to the implementation of the Central American Single Customs Code (CAUCA) and its regulations for electronically transmitting customs declarations, the integration of computer systems and the use of electronic signatures is particularly highlighted. Specifically, the implementation of the Central American Single Customs Form (FAUCA)[11] is an example of best practice in the issuance of certificates of origin (UNCTAD, 2016b).

[11] It consists of an export form for the country of origin and an import form for the country of destination. It provides in advance the necessary information to pay the taxes that correspond to the good. It is considered a certificate of origin.

Figure 9
Levels of implementation of measures on cross border paperless trade in Latin America and the Caribbean, 2017
(Percentages and number of countries in each level of implementation)



Source: ECLAC (2017), based on the Global Survey on Trade Facilitation and the Application of Paperless Trade.

When the main obstacles to the implementation of trade facilitation measures were reviewed, the results showed that the biggest problems are the lack of trained human resources and poor coordination among government agencies. This shows the importance of promoting technical assistance in these fields and the institutional complexity that these types of programs demand.

It is important that the countries of the region pay attention to the promotion of the electronic single window (ESW), along with ensuring laws and regulations on electronic transactions that allows the promotion of paperless trade between countries. Governments must recognize digital certificate authentication authorities to conduct cross-border business transactions. They should also promote the electronic exchange of data between countries on trade, particularly the issuance of electronic certificates of origin and sanitary and phytosanitary certificates.

B. Postal performance

Postal performance is essential to the promotion of electronic commerce and their performance can facilitate the deployment of this activity, while at the same time it can be an opportunity for growth. The United Nations Universal Postal Union (UPU), has built an index about postal development (2IPD), which reviews the evolution of these services worldwide, covering 170 countries. The index consists of the analysis of data, statistics, and surveys collected by UPU (more than 3 billion records of tracking of orders and 100 statistical indicators). This analysis allows the comparison of postal service developments in four dimensions: reliability, scope, relevance, and resilience. To improve their performance in the index, national postal services must increase their operational efficiency and quality of service (reliability), strengthen their connectivity with global supply chains (scope), diversify their portfolio beyond the traditional segments of postal services (relevance) and innovate and adapt their business models to the current business environment (resilience) (UPU, 2016).

Out of the 33 countries in Latin America and the Caribbean analysed by the UPU index, none has a high rating (above 75 points), and only Brazil has an upper middle rating (50), while 14 countries have a lower middle rating, and the remaining 18 have a low rating. According to the UPU, the case of Brazil is explained in part because it achieves a better global postal connection and has a more diversified portfolio of services. In recent years, the number of postal transactions (physical and financial) per capita in Brazil remained between 10 and 100 times higher than the levels observed among their regional peers (UPU, 2016).

Table 3
Integrated Index for Postal Development (2IPD), classification for Latin America and the Caribbean, 2016

Country	Index value	Rating
Brazil	55.00	Upper middle rating
Colombia	44.19	Lower middle rating
Chile	44.15	Lower middle rating
El Salvador	43.66	Lower middle rating
Trinidad and Tobago	40.05	Lower middle rating
Jamaica	39.73	Lower middle rating
Costa Rica	37.32	Lower middle rating
Barbados	32.87	Lower middle rating
Uruguay	30.48	Lower middle rating
Mexico	29.51	Lower middle rating
Honduras	28.86	Lower middle rating
Aruba, Curazao, St. Maarten	28.34	Lower middle rating
Peru	28.24	Lower middle rating
Ecuador	26.34	Lower middle rating
Saint Kitts and Nevis	26.01	Lower middle rating
Argentina	24.83	Low rating
Bahamas	23.15	Low rating
Dominican Republic	23.13	Low rating
Granada	22.66	Low rating
Belize	21.93	Low rating
Paraguay	19.60	Low rating
Cuba	19.26	Low rating
Plurinational State of Bolivia	17.36	Low rating
Panama	17.29	Low rating
Suriname	15.59	Low rating
Antigua and Barbuda	15.10	Low rating
Guyana	13.51	Low rating
Bolivarian Republic of Venezuela	12.74	Low rating
Santa Lucia	11.39	Low rating
Haiti	8.07	Low rating
Dominica	7.58	Low rating
Nicaragua	6.10	Low rating
Saint Vincent and the Grenadines	5.88	Low rating

Source: Universal Postal Union (2016), Integrated Index for Postal Development (2IPD).

When reviewing the score by region of the postal development index (2IPD), index value for Latin America and the Caribbean is 24.6, the lowest score. National postal couriers in the region must take these into account and develop strategies to improve the operation of their postal services, improving their operational efficiency, reinforcing their connectivity with global logistics chains, diversifying their portfolio of products and services beyond the traditional segments and adapting its economic model to a trade context in permanent transformation.

Table 4
Integrated Index for Postal Development (2IPD)

	Index 2IPD	Reliability	Reach	Relevance	Resilience
World	38.6	47.8	43.4	11.6	50.2
Industrialized economies	67.4	79.4	68.2	44.3	66.1
Eastern Europe and CIS	55.1	74.7	58.7	12.2	67.5
Asia-Pacific	38.9	52.0	47.7	13.3	41.0
Middle East	27.5	33.4	37.3	0.6	41.4
Africa	25.4	30.9	26.5	0.1	46.5
Latin America and the Caribbean	24.5	26.3	31.1	2.9	41.6

Source: Universal Postal Union (2016), Integrated Index for Postal Development (2IPD).

C. Online Consumer Protection

One of the main obstacles for online shopping is the lack of confidence. These sociocultural barriers are extremely significant in electronic media due to geographical distances and the lack of direct contact in these transactions. In many cases, consumers have concerns related to the security of financial information, Internet theft, and fraud. On the other hand, the cross-border nature of electronic commerce has become a challenge in terms of solving complaints and disputes between buyers and sellers, many of whom believe that there is a very high cost in resolving these situations[12]. Legal uncertainty in terms of contracts, conditions, and delivery guarantees are barriers to the adoption of electronic commerce.[13]

The regulatory frameworks for consumer protection have been widely adopted in Latin American and the Caribbean. For example, laws have already been enacted in 18 countries, of which 11 have applied Resolution 39/248 on the Guidelines for Consumer Protection approved by the United Nations General Assembly[14], while only 2 countries have not enacted the legislation in the matter and they have not even drafted any bills (UNCTAD, 2016b). The guidelines are applicable to goods and services produced in the country and to imports, and are intended to build trust in electronic commerce. In this way, the countries are committed to ensuring that consumers and businesses are informed and aware of their rights and obligations in the digital market. The guidelines also call for observing the recommendations of the Guidelines for Consumer Protection in the Context of Electronic Commerce of the Organization for Economic Co-operation and Development (OECD).

The OECD (2000)[15] recommendations provide basic principles to guide governments to review, formulate, and implement regulatory frameworks and policies that protect consumers in the context of electronic commerce, in addition to guiding companies in self-regulatory mechanisms and fair business practices. These principles seek to promote the provision of transparent and effective information about companies and products offered online, as well as details about costs, and the terms and conditions of electronic transactions. The guidelines refer to the fulfilment of criteria so that advertising and marketing respect the interests of consumers. The areas referred to the mechanisms of secure payments, the resolution of disputes and compensation for damage, as well as the promotion of privacy, education, and awareness are also part of these recommendations.

[12] According to Consumer Barometer (2016), the three main reasons why people do not make cross-border purchases on the Internet are local sites that meet their needs, there is no trust in online stores abroad, and returns are expensive.

[13] The absence of full harmonization of national consumer protection legislation may explain why some suppliers hesitate to sell their products in different markets (Martens, 2013).

[14] The guidelines were approved by the General Assembly in its Resolution 39/248 of 16 April 1985, subsequently expanded by the Economic and Social Council in its Resolution 1999/7 of July 26, 1999, and revised and approved by the General Assembly in its resolution 70/186 of 22 December 2015.

[15] The OECD recommendations only apply to electronic commerce between businessmen and consumers, and not to business-to-business transactions.

In 2014, as part of the general review of the guidelines presented on electronic commerce, the OECD issued an orientation guide for policies on the consumption of intangible digital products. This review is based on the importance of considering the growing expansion of digital markets for digital content products[16] due to factors such as the diversification of channels that allow the acquisition of these types of products —besides to traditional websites and e-commerce platforms— such as digital television, mobile devices, and social networks. The problems identified include the disclosure of inappropriate information, deceptive or unfair business practices, the collection, use and exchange of personal data, inadequate mechanisms for dispute resolution and redress, and the possibility of unauthorized charges associated with the use of applications and online games.

The guide on intangible digital products complements the guidelines issued on electronic commerce in several aspects. One of these is the provision of clear and timely information on the conditions of acquisition, access, and use of digital content. Other aspects refer to the privacy and security of personal data and the request for expressed consent in its collection, use, and dissemination. The guide also notes the importance of providing information about changes in testing periods or automatic renewal of contracts, subscriptions and online purchases, and the promotion of dispute resolution and repairs. Another issue relates to advertising aimed at children, since it may encourage them to purchase products and services without the consent of parents or guardians.[17] Finally, improving the skills and digital knowledge of consumers to defend their rights is also pointed out as a topic to be addressed by governments and companies in this guide on intangible digital products (OECD, 2014).

In MERCOSUR, agreements to promote and complement efforts on consumer protection on the Internet have facilitated regulatory harmonization between Argentina, Brazil, Paraguay, Uruguay, Venezuela, and Bolivia. Of relevance there is Resolution No. 21/04 on the Consumers' Right to Information in Commercial Transactions Made via the Internet. This resolution guarantees the provision of clear, accurate, sufficient and accessible information about the service provider, the product or service acquired, and other electronic transactions. In general terms, it considers the online information principle of the recommendations on consumer protection in electronic commerce issued by the OECD.[18]

In addition, in the field of self-regulation, various chambers and national associations have developed codes of conduct and trust seal schemes related to electronic commerce. The eConfianza seal of the Latin American Institute of Electronic Commerce (eInstituto) stands out, which has joined the efforts of the Argentine Chamber of Electronic Commerce (CACE), the Chamber of Commerce of Santiago (CCS), the Venezuelan Chamber of Electronic Commerce (CAVECOM) -E), the Brazilian Chamber of Electronic Commerce (Cámara e-net), the Mexican Internet Association (AMIPCI), the Paraguayan Chamber of Electronic Commerce (CAPACE), the Peruvian Chamber of Electronic Commerce (CAPECE), the Dominican Chamber of Commerce, Dominican Chamber of Electronic Commerce, Inc (CADOLEC), the Chamber of Commerce of Lima (CCL), the Colombian Chamber of Electronic Commerce (CCCE), the Chamber of Commerce of Guayaquil (CCG), and the Ecuadorian Electronic Commerce Corporation (CORPECE), which have a system of cross recognition of trust seals (UNCTAD, 2016b).

[16] According to the OECD, digital content products refer to products that are acquired through the Internet and mobile platforms, and that are received in electronic formats and through electronic transactions (electronic commerce), without the need for a monetary payment. The guide distinguishes between products that involve a monetary cost and those that do not.

[17] Although that in most countries children do not have the legal capacity for payment commitments, in many cases they are able to purchase digital content without the knowledge of their parents or guardians.

[18] They also highlight Resolution No. 45/06 on Consumer Protection and Deceptive Advertising and Decree No. 10/96 – MERCOSUR Santa Maria Protocol 10/96 on International Jurisdiction in the field of consumer relations.

Table 5
Review of international frameworks on consumer protection in the field of electronic commerce

United Nations Guidelines for Consumer Protection (UNCTAD, 2016)	Guidelines for consumer protection in the context of electronic commerce (OECD, 2000)	Consumer Policy Guidance on Intangible Digital Content Products (OECD, 2014)
Application area Transactions between companies and consumers, including the provision of goods and services to consumers by state-owned companies.	Application area E-commerce between entrepreneurs and consumers, excludes transactions between companies.	Application area Intangible digital products that are acquired by Internet platforms and mobile networks and that are received in electronic format and through electronic commerce.
Guidelines on electronic commerce	General Principles	Issues related to consumer protection policies
• Design transparent and effective policies that guarantee a degree of protection not inferior to that granted in other forms of commerce • Include electronic commerce in consumer protection policies and guarantee information and awareness about rights and obligations • Examine and adapt international guidelines and standards	• Transparent and effective protection • Fairness in business, advertising, and marketing practices • Online information • Information about the company • Confirmation procedures • Dispute settlement and damage repair • Alternative mechanisms for the resolution of disputes and reparation of damage • Privacy • Education and awareness	• Conditions of acquisition, access and use of digital content products • Privacy & Security • Fraudulent, deceptive, and unfair business practices • Children • Conflict resolution • Digital competitiveness

Source: ECLAC based on UNCTAD (2016), Guidelines for Consumer Protection, OECD (2000), Guidelines for consumer protection in the context of electronic commerce and OECD (2014), Guidelines for targeting consumer policies of intangible digital products.

In terms of online consumer protection, countries should adopt regulatory frameworks on consumer protection in the context of electronic commerce, recognizing the United Nations' guidelines. They should also move towards the adoption of common principles and guidelines to address the challenges involved in the consumption of intangible digital products and promote regional coordination on self-regulatory mechanisms in electronic commerce.

D. Digital financial inclusion and means of online payment

It is imperative to take advantage of the opportunities that digital technology offers to expand the scale and reach of financial services. New technology-based companies focused on providing innovative financial services (known as FinTech) are disrupting the traditional banking value chain, including payment services, credit, financial management, and capital markets, among other segments. The incentives are massive since in many segments market opportunities still exist. It is estimated that the global investment in FinTech reached US$12 billion in 2016 (FSB, 2017). According to McKinsey (2015) payments are the fastest growing segment.

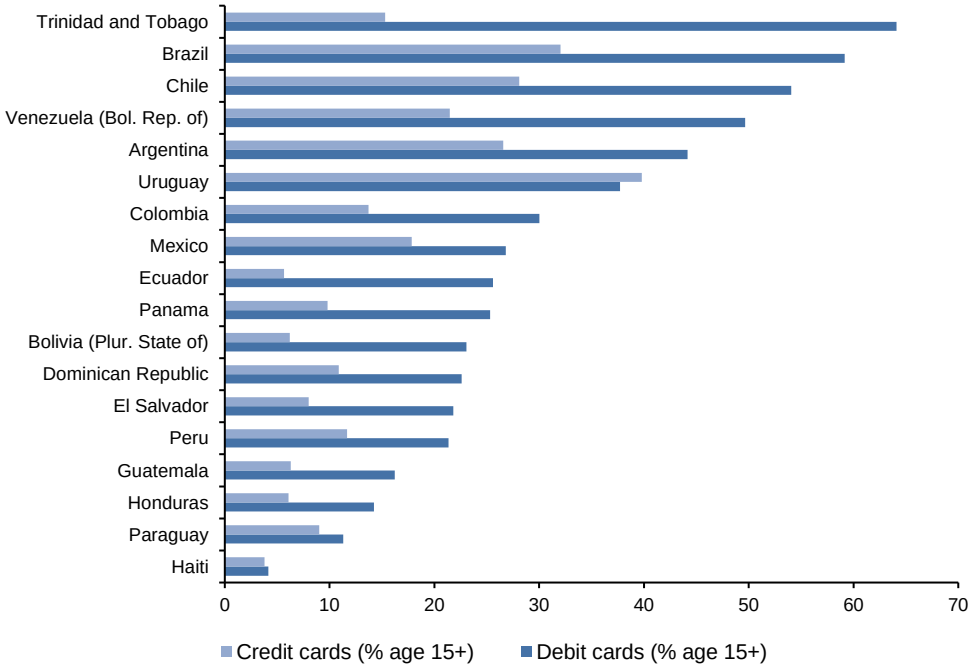
Table 6
Customer segments and products of the 350 leading companies in FinTech, globally, 2015
(Percentage of total)

Customer Segments	Account Management	Loans and financing	Payments	Financial assets and capital markets
Retail	10	14	25	13
Small and medium companies trade	3	9	12	4
Large companies trade	2	1	6	2

Source: McKinsey (2015), The Fight for the Customer: McKinsey Global Banking Annual Review.

Access to payment services is key to promoting electronic commerce. The most popular payment methods to purchase goods and services online are credit and debit cards (Nielsen, 2015), however, these means of payment have low penetration rates. The difference between countries in the use of credit and debit cards reaches 36 and 60 percentage points, respectively. According to the most recent data accessible, on average, 18% of the population in Latin America and the Caribbean claims to use credit cards and 28% debit cards (World Bank, 2014).

Figure 10
Latin America and the Caribbean: percentage of credit and debit cards used in the last year, 2014



Source: World Bank (2017), Global Finance Inclusion Database.

The financial sector and especially the payments market have experienced a significant expansion in recent years not only globally but also at regional level. Revenue from global payments grew 9% in 2014, compared to 4% between 2011 and 2013, and is expected to grow 6% by 2019. In Latin America, this revenue is expected to grow 9% between 2014 and 2019. However, the expansion of these services is mainly due to an increase in volume, and not to an increase in efficiency (McKinsey & Company, 2015). In addition, the costs of financial intermediation have not reduced in the last decades. Thus, improvements in the use of digital technologies have not been transmitted to end users (Philippon, 2015, and Bazot, 2013).

The payments segment faces disruptive factors on several fronts related to digitization. One of those is the appearance of non-banking actors that offer services in the payment media industry, such as Apple (Apple Pay), Google (Android Pay) or Samsung (Samsung Pay). Other companies are offering cross-border money transfer systems peer-to-peer (P2P), such as Transferwise[19]. As these innovations grow, banks may have difficulties maintaining margins. Regulations such as the European Payments Services Directive[20] can be a catalyst for innovation (McKinsey, 2015). Part of the objectives of this directive is to achieve a more integrated internal market for electronic payments in the European Union (see box 1).

[19] It is a money transfer service between individuals developed in the United Kingdom in January 2011.
[20] Directive (EU) 2015/2366 on payment services throughout the EU.

Box 1
Summary of the EU Directive 2015/2366 on payment services

What is the purpose of the directive?
- Provide the legal basis for an improved development of a more integrated internal market for electronic payments within the EU.
- Establish comprehensive rules for payment services, with the aim of making international payments (within the EU) as easy, efficient, and secure as payments in a single country.
- Open markets to new entrants, increasing competition, providing greater supply and better prices for consumers.
- Provide the necessary legal platform for the single area of European payments (SEPA).

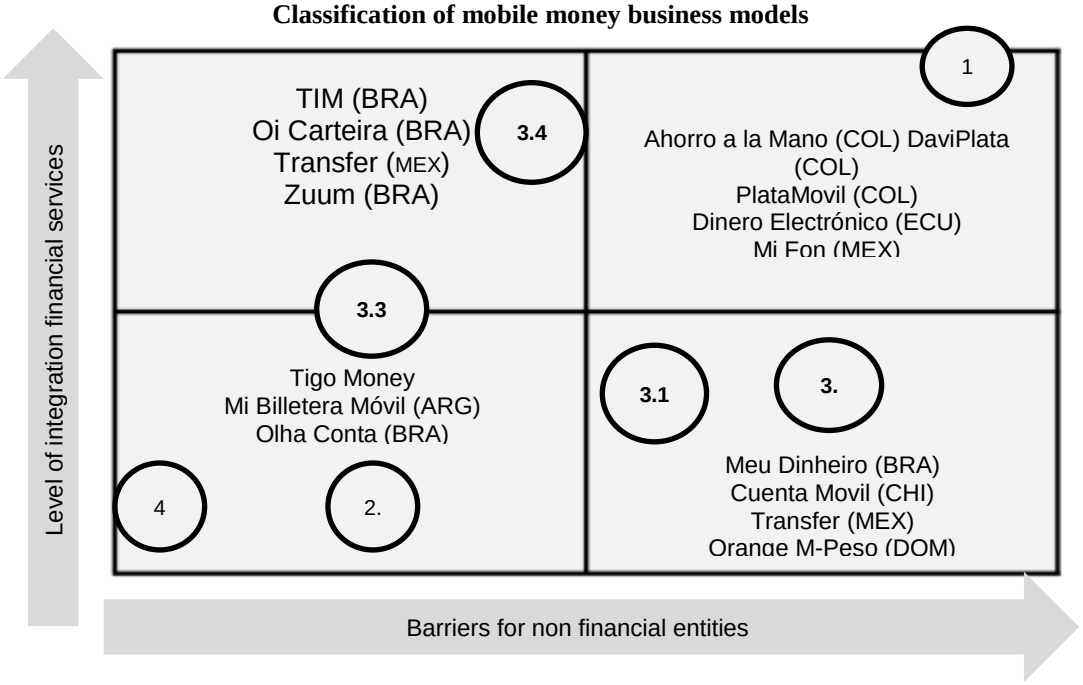
Key points
- The Directive seeks to improve the current EU rules for electronic payments. It takes into account emerging and innovative payment services, such as the Internet and mobile payments.
- The Directive establishes rules relating to: strict security requirements for electronic payments and the protection of consumers' financial data, guaranteeing secure authentication and reducing the risk of fraud; more transparency about the conditions and information requirements for payment services; the rights and obligations of users, and payment service providers.

Source: European Union (2017), EUR-Lex. Access to European Union Law, "Revised rules for payment services in the EU".

On the other hand, mobile payments have experiences a rapid expansion in the region, and have been characterized by many business models. According to Lachowicz (2016), at least 36 services are offered in 18 countries in the region, which are provided by a banking entity, a mobile operator, an independent actor or through a collaborative model. Some common characteristics are the definition of maximum limits to store transfer money (for the prevention of money laundering and prevention of the financing of terrorism) and the flexibility to request an account (designed to meet the needs of individuals with lower resources). Also, rates are based on transactions fees (P2P or service payments). The entities that offer these services require backup mechanisms (trust fund or deposit insurance).

Regulatory differences in the region affects business models in the mobile money segment. The greater the barriers for non-financial entities to entry the market, the higher the participation of banking entities or traditional players in the industry; the same relationship is presented in terms of financial integration. There are different regulatory models. The most restrictive ones present a greater participation of banks (Type 1) or are initiatives led by mobile network operators (Type 2). In a market with fewer barriers and greater openness, there are independent service providers (Type 4). The remaining models are those of a collaborative type that have combinations of actors (Type 3): alliances of mobile operators with banking institutions (Type 3.1) and banks associated with independent service providers (3.2). Other collaborative models (upper left quadrant) are cooperation’s between mobile network operators and payment service providers (Type 3.3). Banks, mobile network operators, and payment service providers participate in the last collaborative model (Type 3.4) (Lachowicz, 2016).

Diagram 1
Classification of mobile money business models



Source: M. S. Lachowicz (2016), Mobile Payments in Latin America and the Caribbean.

Some of the key issues on the regulation of digital financial inclusion are related to the problems of the agents: rules against money laundering (AML) and financing terrorism (CFT), the regulation of digital money, consumer protection, regulation of payment systems, and competition. These issues fall within the scope of various authorities, which requires effective communication and collaboration between regulators. The main risks associated with these models are lending risk, operational (such as technological failure or lack of reliability), compensation and financial crimes, including fraud, as well as money laundering and financing terrorism (GPFI, 2014).

The Group of the Twenty (G-20) has recognized the role of digital technologies for financial inclusion and its importance in moving towards an inclusive global economy. In this regard, it has proposed to take concrete actions, under the guidance of international financial organizations. In particular, the G20 have committed to help developing and low-income countries to take measures to promote digital financial inclusion and compliance with the 2030 Agenda. In this way, a set of guiding principles was approved, highlighting the importance to strengthen international cooperation, the exchange of experiences, and learning mechanisms to promote digital financial inclusion.

In this framework, it is important that countries take into account these principles in the design of policies and regulations with the objective of promoting financial inclusion through digital technologies. On the other hand, it is important to observe specific agreements that seek greater integration of the payments market at a regional level, allowing innovation and the improvement of traditional payment systems, remittances, and the participation of SMEs in the digital economy.

Box 2
Principles for digital financial inclusion

1. Promote a digital approach to financial inclusion

Promote digital financial services as a priority to develop inclusive financial systems, through coordination, monitoring and evaluation of strategies and action plans.

2. Balance innovation and risk to achieve financial inclusion

Balance innovation to achieve digital financial development, identifying, evaluating, monitoring, and managing new risks.

3. Provide a legal and regulatory enabling framework

Provide a legal and regulatory framework for digital financial inclusion, taking into account international standards and guidelines.

4. Expand the infrastructure ecosystem for digital financial services

Expand the ecosystem of digital financial services -including the information and communications infrastructure- for the safe, reliable, and low-cost provision of services to all relevant geographical areas, especially underserved rural areas.

5. Establishment of responsible digital financial management to protect consumers

Establish a comprehensive approach to consumer protection and data protection on issues of relevance to digital financial services.

6. Strengthen awareness and digital and financial skills

Support and evaluate programs that improve financial literacy in light of the unique characteristics, advantages, and risks of digital financial services and their channels.

7. Facilitate the identification of the client for digital financial services

Facilitate access to digital financial services by developing and promoting the development of identification systems for clients, in addition to products and services that are accessible, affordable and verifiable, and that accommodate multiple needs and levels of risk, considering an approach based on the risk and due diligence of the client.

8. Monitor the progress of digital financial inclusion

Monitor progress in digital financial inclusion through comprehensive and robust data measurement and an evaluation system. This system should take advantage of digital data sources and allow interested parties to monitor the supply and demand of financial services, as well as to evaluate the impact of programs and reforms.

Source: Global Partnership for Financial Inclusion (GPFI) (2016), G20 High-Level Principles for Digital Financial Inclusion.

IV. Cybersecurity

While there is a consensus on threats in cybersecurity, addressing these challenges is a complex issue that requires actions in various policy areas and cooperation efforts. Recent incidents of cybersecurity, including massive malware attacks worldwide, have shown vulnerabilities in the digital area.[21] These illicit activities threaten security and privacy on a large scale, with a significant cost to the economy and society.

The global cybersecurity index (GCI) developed by the International Telecommunication Union (ITU) measures the level of commitment in this field, based on a series of individual indicators about measures taken by countries about legal, technical, organizational, capacity building and cooperation issues. The indicators are based on a survey that reviews laws, regulations, computer security response teams (CSIRT), policies, strategies, standards, certifications, professional training, raise awareness, and collaboration associations. According to the 2017 version of the index, 20 of the 33 countries of Latin America and the Caribbean are in a basic stage in relation to their cybersecurity policies and strategies, only 13 countries are in a stage of maturation and none reach an advanced stage (as for example, the United Kingdom, Canada, and Japan). With great heterogeneity between countries, the greatest deficiencies relate to technical, organizational and training aspects (ITU, 2017).

The countries of the region that are best positioned are Mexico, Uruguay, and Brazil. When comparing the indicators among regions, the biggest difference is related to the measures adopted in organizational (strategy, responsible agency, metrics), and cooperation aspects (national cooperation, multilateral treaties, public-private partnerships, interagency associations, participation in international forums). The index also shows deficiencies in technical issues (establishment of CSIRT, adoption, and certification of standards on cybersecurity, online child protection, among others), and capacity development (public and private research and development of standards, training and certification of professionals and organizations). The best performance is in the legal field (legislation on cybercrime), although in this matter there are considerable challenges.

Regarding the cybercrime legal framework, according to UNCTAD (2016b) only two countries (Panama and the Dominican Republic) have signed the Council of Europe Convention on Cybercrime and have modified their functional and technical laws in accordance with this instrument; in 17 countries there are laws that classify some kinds of cybercrimes, while in one case there is no regulation. Regarding Information Security; 13 countries have a Cyber Incidents Response Centers (CSIRT, CERT or CIRT) and have adopted the recommendations of the Inter-American Committee against Terrorism (CICTE) of the Organization of American States (OAS).

[21] In one day, WannaCry infected more than 230,000 computers in more than 150 countries affecting public and private services (BBC, 2017). Cyberattacks on industrial systems and critical infrastructures increase on a yearly basis (CNN, 2017).

Table 7
Latin America and the Caribbean: ranking in the global cybersecurity index (GCI)

Initiating		Maturing	
Country	Ranking	Country	Ranking
Dominica	163	Paraguay	87
Haití	161	Costa Rica	86
Honduras	157	Jamaica	85
Santa Lucia	156	Chile	81
Cuba	153	Venezuela (Bolivarian Republic of)	80
San Kitts and Nevis	151	Peru	79
Trinidad and Tabago	141	Ecuador	66
Guatemala	138	Argentina	63
Granada	137	Panama	62
Bolivia (Plurinational State of)	134	Colombia	46
Surinam	132	Brazil	38
Bahamas	129	Uruguay	29
Nicaragua	125	Mexico	28
Dominican Republic	122		
Antigua and Barbuda	117		
Belice	116		
Saint Vincent and the Grenadines	114		
El Salvador	108		
Guyana	98		
Barbados	95		

Fuente: ITU (2017), Global Cybersecurity Index.

At the sub regional level, there are several cooperation initiatives: i) The annual action plans of the South American Defence Council of the Union of South American Nations (UNASUR), with this reference a working group has been formed to evaluate the feasibility of establishing regional policies and mechanisms to face cyber and computer threats in the field of defence; ii) The Conference of Ministers of Justice of the Ibero-American Countries (COMJIB) signed the Ibero-American Cooperation Agreement on Research, Assurance and Secure of Evidence in Cybercrime to strengthen cooperation to obtain evidence for fighting cybercrime; iii) The "Special Declaration 15: On governance processes on the Internet" adopted at the III Summit of the Community of Latin American and Caribbean States (CELAC) held in Costa Rica in January 2015, states in one of its sections "*iii) its commitment to promote actions and strategies to strengthen cybersecurity and prevent cybercrimes* ... "(UNCTAD, 2016b).

Among the regional cooperation initiatives in this area, it is worth mentioning the Cybersecurity Program of the Secretariat of the Inter-American Committee against Terrorism (CICTE) of the Organization of American States (OAS), based on the Comprehensive Inter-American Strategy to Combat Cybersecurity Threats[22] adopted by the General Assembly of the OAS in 2004. Among its objectives are the establishment of incident response teams (CSIRT) in each country, the creation of a hemispheric alert network that provide technical training to personnel working in cyber security in governments, the development of national strategies on cybersecurity, and the development of a culture that allows the strengthening of cybersecurity in the hemisphere.

There are considerable advances in these aspects, however, the legal, organizational and technical deficiencies are still evident. There is still much to be done, considering the increase in cybercrimes that have exploit digital vulnerabilities with high costs and the undermining of confidence in digital tools. In particular, countries, should strengthen regional cooperation through multilateral agreements, public-private partnerships, and their participation in international forums.

[22] Resolution AG / RES. 2004 -XXXIV-O / 04.

V. The digital economy in regional economic integration agreements[23]

The importance of the digital economy for growth and social development is recognized both at country level —which is reflected in national strategies and plans for the digital economy— and at regional and sub regional economic forums and trade alliances that designate increasingly more relevance to digital factors in their agendas. The EU is exemplary in this regard, in which the creation of a single market has taken place over a decades-long trajectory of economic, social, and political integration based on treaties and materialized in a common set of laws, institutions, and norms. However, although national barriers to a single market have been eliminated in the physical world, there are considerable challenges in the digital markets.[24]

The countries of the region do not have a significant socioeconomic integration and lack a sole Pan-American institutional framework with binding powers. All the countries of the region are part of bilateral agreements to promote trade and collaboration, regional economic forums and other multilateral organizations. Most are members of one or more regional or sub regional trade blocks that seek to eliminate tariffs and non-tariff barriers to facilitate trade relations among their members. Approaches to trade vary considerably among these alliances not only in terms of their central mission, membership, and organization, but also in terms of the historical and political period in which they were established.

The following table shows the participation of 20 Latin American and Caribbean countries in selected regional or sub-regional entities. While some, such as Mexico, Chile or Colombia, are part of several groups,

[23] This chapter is based on Cullen International (2018), "Regional and Sub-Regional Approaches to the Digital Economy: Lessons from Asia Pacific and Latin America," document prepared by Cullen International for CAF - Development Bank of Latin America, unpublished.

[24] According to the European Commission: "A Digital Single Market is one in which the free movement of goods, persons, services and capital is ensured and where individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence. Achieving a Digital Single Market will ensure that Europe maintains its position as a world leader in the digital economy, helping European companies to grow globally. Europe has the capabilities to lead in the global digital economy but we are currently not making the most of them. Fragmentation and barriers that do not exist in the physical Single Market are holding the EU back." (European Union, 2015).

others are only part of large multilateral organizations such as ECLAC or the OAS, and have little or no presence in the sub regional trade agreements.[25]

Table 8
Membership in selected regional and subregional entities

Country	OAS	ECLAC	CAN	CARICOM	ALADI	APEC	SICA	MERCOSUR	TLCAN	Mesoamerica Project	Pacific Alliance	TPP
	1948	1948	1969	1973	1980	1989	1991	1991	1994	2008	2011	2016
Argentina	✓	✓			✓			✓				
Belize	✓	✓		✓			✓			✓		
Plurinational State of Bolivia	✓	✓	✓		✓			✓				
Brazil	✓	✓			✓			✓				
Chile	✓	✓			✓	✓					✓	✓
Colombia	✓	✓	✓		✓					✓	✓	
Costa Rica	✓	✓					✓			✓		
Cuba	✓[a]	✓			✓							
Dominican Republic	✓	✓					✓			✓		
Ecuador	✓	✓	✓		✓							
Guatemala	✓	✓					✓			✓		
Honduras	✓	✓					✓			✓		
Mexico	✓	✓			✓	✓			✓	✓	✓	✓
Nicaragua	✓	✓					✓					
Panama	✓	✓			✓		✓					
Peru	✓	✓	✓		✓	✓					✓	✓
Paraguay	✓	✓						✓				
El Salvador	✓	✓					✓					
Uruguay	✓	✓			✓			✓				
Bolivarian Republic of Venezuela	✓	✓			✓			✓				
Canada	✓	✓				✓			✓			✓
United States of America	✓	✓				✓			✓			✓

Source: Cullen International (2018), Regional and Sub regional Approaches to the Digital Economy: Lessons from Asia-Pacific and Latin America, document prepared by Cullen International for CAF - Development Bank of Latin America, unpublished.
[a] On 3 June 2009, the Ministers for Foreign Affairs of the Americas adopted Resolution AG/RES. 2438 (XXXIX-O / 09), which resolves that Resolution 1962, which excluded the Government of Cuba from participating in the inter-American system, has no effect on the Organization of American States (OAS). The 2009 resolution declares that the participation of the Republic of Cuba in the OAS will be the result of a dialogue process initiated at the request of the Government of Cuba, and in accordance with the practices, purposes, and principles of the OAS.

All regional and sub regional associations have worked on issues related to the digital economy. The following is a summary of the adopted provisions and activities carried out by the TTP, APEC, CARICOM, the Mesoamerica Project, SICA, the Caribbean Community, the Pacific Alliance, and Mercosur. Among the entities analysed, the most recent ones —for example, the TPP and the Pacific Alliance— put special emphasis on trade and development aspects related to the Internet and the digital economy.[26]

[25] Although not part of Latin America, the United States and Canada are members of entities in which one or more Latin American countries participate, including the Organization of American States (OAS), the Economic Commission for Latin America and the Caribbean (ECLAC), the Free Trade Association of North America (NAFTA), the Asia-Pacific Economic Cooperation (APEC), and the Trans-Pacific Partnership (TPP).

[26] In the annex, a comparative table of the main activities carried out by respective associations is presented.

A. The Trans-Pacific Agreement

The objective of the TPP is to promote trade and economic relations between the signatory nations by reducing or eliminating tariffs and customs taxes and formulating guidelines on economic policies and regulation to encourage electronic commerce and trade in digital goods and services[27]. Among its 30 chapters covering trade and non-trade issues, some explicitly consider e-commerce, intellectual property, and competitiveness. The Agreement includes obligations to promote the digital economy through a free and open Internet and trade without borders, through specific provisions for the digital environment, including issues of security and privacy, electronic commerce of digital goods and services, copyright, regulation and application of patents.

Table 9
TPP provisions on telecommunications and electronic commerce

Thematic area	Provisions
Free and open internet	Consumers should be able to access the content and applications of their choice when they are online. Promote a free and open Internet that allows the creation of new online services and the development of electronic commerce.
Regulations of telecommunications networks	Commitments to guarantee, under non-discriminatory, reasonable and transparent conditions, access and interconnection, granting of licenses, allocation of scarce resources and international roaming
Cybersecurity	Members will work to share information about threats and help build capacity in cybersecurity to prevent cyber-attacks and malware distribution.
Intellectual Property	Copyright: provisions that establish the protection of copyright for works, interpretations and software. Requirements to establish or maintain a safe harbour framework for Internet Service Providers (ISP).
	Patents: strengthen the protection of patents on next-generation innovation, based on the WTO TRIPS Agreement and international best practices.
	Trademarks: protection of trademarks and other symbols.
	Industrial designs: guarantees that companies do not have to share source codes, trade secrets or substitute local technology for their products and services to enter a new market.
	Rules that prohibit countries from requiring companies to transfer their technology or production processes.
	Execution systems: criminal procedures and criminal sanctions for the theft of trade secrets (including cyber theft), counterfeiting of trademarks and piracy of copyright or related rights.
Standards and technical standards	Transparent and non-discriminatory rules for the development of technical regulations and standards. Cooperation to ensure that technical regulations and standards do not create unnecessary barriers to trade.
	Possibility for the public to comment on the technical regulations and the proposed standards.
	Ensure a reasonable interval between the publication of technical regulations and their entry into force, so that companies have enough time to comply with the new requirements.
	Specific regulatory approaches common throughout the TPP region in information and communication technology products.
Consumer protection	Member countries must adopt and maintain consumer protection standards (including privacy) to offer consumers a reliable environment for electronic commerce.
Competition policies	The parties share the interest of ensuring a framework of fair competition in the region through rules that require the parties to maintain legal regimes that prohibit anti-competitive commercial conduct, as well as fraudulent and deceptive commercial activities that harm consumers.
	They agree to establish or maintain authorities responsible for the application of national competition laws and regulations.

[27] The TPP was signed in February 2016, by 12 countries bordering the Pacific Ocean (Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, United States, and Vietnam), but did not enter into force until January 2017. The President of the United States signed a Presidential Memorandum to withdraw the United States from the TPP. There are two ways for this agreement to take effect: i) all countries ratify the agreement (in that case, the TPP enters into force 60 days after the last member's ratification); or ii) at least six original signatories ratify the agreement, representing 85% of the GDP of the original twelve nations (after two years since the signing and if the first option did not occur). The TPP has been ratified by New Zealand and Japan. Information updated up to the date of publication of this document.

Table 9 (concluded)

Digital customs and customs treatment of digital goods	Prohibition of customs duties for digital goods and services. Commitments on the facilitation of customs and commercial procedures, including paperless trade, using digital customs forms.
Cross-border investment and digital services	Strong investment commitments and cross-border services, allowing providers to offer cloud computing and other technology related services in all TPP countries. The parties share an interest in accessing the large public procurement markets of the others through transparent, predictable, and non-discriminatory rules.
Non-discrimination	Digital products from partner countries can not have competitive disadvantages in any market.
No location barriers	Access to networks and efficient data processing, including the rules of not requiring TPP companies to build data centers to store data as a condition of operating in a TPP market. Do not require the transfer or access to the source code of the software.
Choice of technology options and encryption solutions	Choice of technology, to ensure that companies are not forced to use local technology. Use of electronic signature and authentication methods in electronic payments.
Cross-border data flows	Specific provisions designed to protect the free flow of data, subject to reasonable protection measures (protection of consumers' data when they are exported, ensuring that there are no discriminatory and protectionist barriers).

Source: Cullen International (2018), "Regional and Subregional Approaches to the Digital Economy: Lessons from Asia-Pacific and Latin America", document prepared by Cullen International for CAF - Development Bank of Latin America, unpublished.

B. The Asia-Pacific Economic Cooperation Forum

The Asia-Pacific Economic Cooperation Forum —a 30-year-old scheme established between 21 economies bordering the Pacific Ocean (Mexico, Chile, and Peru in Latin America)— is an example of a regional commitment to the digital economy. This multilateral economic forum is the only international intergovernmental group committed to reducing barriers to trade and investment without requiring its members to assume legally binding obligations. Thus, it seeks to achieve its goals by promoting dialogue and reaching decisions based on consensus, giving equal weight to the opinions of all its members.

APEC recognizes the role of the Internet economy for growth and development and is committed to the goal of creating an Asia-Pacific region that is connected and integrated by year 2025 (APEC, 2014). Over the years, cooperation among its members has increased with a reduction of trade barriers, including for electronic commerce, and the promotion of innovation and standardization of ICTs.

Most of regional connectivity initiatives in APEC is developed by the Telecommunications and Information Working Group (TEL WG). This group and the Ad Hoc Steering Group on Internet Economy (AHSGIE) seek to propose and implement projects that address the priorities established by telecommunications and information ministers. Established in 1990, the TEL WG promotes cooperation, the exchange of information and the development of effective ICTs policies and regulations in the region. It also seeks social and economic development through the effective use of ICTs and the promotion of a safe and reliable ICT environment. The TEL WG has three groups dealing with liberalization, development, and security.

In 2015, APEC adopted an action plan for the telecommunications sector towards 2020, which includes specific actions and possible initiatives, including innovation, and value creation in ICTs, access to broadband, digital literacy, greater adoption of ICTs in the APEC economies, greater resilience of internal critical infrastructure and cybersecurity (APEC, 2015a).

Several of its projects are public and private initiatives build in collaboration with international organizations, such as the International Telecommunications Union (ITU), the Organization for Economic Co-operation and Development (OECD), the Asia-Pacific Network Information Center (APNIC), the Internet

Society (ISOC), and the International Telecommunications Users Group (INTUG). In addition, several projects are initiated and directed only by the private sector.

The APEC Committee on Trade and Investment, the Electronic Commerce Steering Group (ECSG) coordinates electronic commerce activities based on the principles established in the 1998 Blueprint for Action on Electronic Commerce (APEC, 1998).

The APEC ECSG has a Data Privacy Subgroup (DPS) that analyses and identifies best practices. The APEC Privacy Framework (2015b) —adopted in 2004 and updated in 2015— deals with deficiencies in the policies and regulatory frameworks on electronic commerce and seeks to ensure that the free flow of information and data across borders is balanced with the effective protection of personal data, as an essential element for trust in online markets. Ministers endorsed the revised standards in Lima, Peru, in November 2016.

In 2005, APEC Ministers approved copyright guidelines that, while not binding, aim to provide guidance on how to reduce online piracy, protect against unauthorized digital copies, and promote a secure environment to promote the continuous growth of electronic commerce.

The policy guidelines of the APEC Industrial Science and Technology Working Group (ISTWG) are set by APEC economic leaders, and implemented by APEC ministers responsible for science and technology. In 2012, it was agreed to extend the mandate of this working group to include innovation policy issues, converting it into the Policy Partnership on Science, Technology, and Innovation (PPSTI) to improve cooperation among the government, the private sector, and the academic world. The PPSTI identifies areas of alignment with international frameworks and reviews member activities, seeking to disseminate best practices and improve regulatory cooperation. It also works to complement and strengthen the work of regional or multilateral organizations, such as the ASEAN Committee on Science and Technology.

C. The Mesoamerica Project and the Central American Integration System

The Mesoamerica Project seeks to strengthen regional integration and promote economic and social development of their countries (Salido J., 2015). Since its creation, the Mesoamerica Project has contributed to the establishment of regional projects and initiatives. In a first phase, its focus was on the physical integration of the electrical, telecommunications, and transport infrastructure. In a second phase, it has promoted initiatives with a high social impact, such as health care and environmental protection.

The pillars of the Mesoamerica Project are:

- Political dialogue: a high-level discussion forum to review regional priorities.
- Regional integration: projects and activities to increase interdependence among member countries.
- Specialization: promotion of specific projects in a regional context.
- Financing: attracting resources from international cooperation agencies and multilateral banks.
- Regional scope: promotion of beneficial initiatives at the regional level.

One of the main initiatives supported by the Mesoamerica Project is REDCA,[28] an infrastructure project co-financed by the Development Bank of Latin America (CAF) which offers neutral support to wholesale telecommunications services with a regional scope. In addition, the Mesoamerican Agenda for the Integration of Telecommunications Services (AMIST) brings together regional and national actors and seeks to strengthen public policies at regional level.[29] It also promotes regional cooperation between regulators and

[28] Red Centroamericana de Telecommunicaciones – Central American Telecommunications Network.

[29] The strategic guidelines for the 2013-2015 identified 5 pillars of the regional strategy: i) infrastructure, development of content, and applications; ii) connectivity and accessibility to reduce the digital divide; iii) regulatory aspects, towards better harmonization; iv) ICT for the protection of the environment; and v) institutional strengthening (El Salvador, Ministry of Foreign Affairs and the Mesoamerica Integration and Development Project, 2013).

telecommunications ministries, in the Mesoamerican Telecommunications Authorities Forum (FMAT), created in 2001. The FMAT has not yet been formalized by the member countries and acts under the regional coordination of El Salvador. Recently, countries have agreed to re-initiate negotiations for the establishment of a Memorandum of Understanding to institutionalize the FMAT.

Eight-member countries of the Mesoamerica Project (Salido J., 2015) are also part of the Central American Integration System (SICA), an institutional framework for regional integration established in 1991 by the Protocol of the Charter of the Organization of Central America (ODECA) or Tegucigalpa Protocol (initially integrated by six Central American countries. Belize and the Dominican Republic joined in 2013).

The main objective of SICA is the integration of Central America and its transformation into a region of peace, freedom, democracy, and development, based on respect and the promotion of human rights. In October 1993, six countries signed the Protocol of the General Treaty on the Economic Integration of Central American (Protocol of Guatemala) by which they ensure, on a voluntary, gradual, progressive, and complementary basis, promote the economic union of Central America. To this end, they formed the Economic Integration Subsystem, whose technical and administrative body is the Secretariat of Central American Economic Integration (SIECA) based in Guatemala (El Salvador, Guatemala, Honduras, and Nicaragua, 1993).

Although the SICA agenda is mainly political, in June 2014, the Heads of State entrusted the General Secretariat to coordinate with the highest national and regional authorities, responsible for the promotion of the information society, the development of a regional strategy and its implementation. Although the proposal was adopted in March 2015, there is no information on whether it was formally implemented. The proposed strategy is aligned with the main objectives and actions established in other relevant international forums in which the member countries of SICA participate (SICA, 2015):

- Sustainable Development Goals (UN)
- World Summit on Information Society (ITU)
- Work plan of the Network of e-Government Leaders of Latin America and the Caribbean (RedGEALC)
- The digital agenda of Latin America and the Caribbean (eLAC - ECLAC)

The objective of having a strategy about the information society is to ensure that SICA members have "an enabling environment to move forward in a coordinated manner, in the implementation of regional initiatives, where dialogue and the exchange of experiences accelerate the establishment of an information society in the region, with tangible benefits for the Central American people" (SICA, 2015, page 3).

D. The Caribbean Community

The roadmap to promote a Single ICT Space was approved in February 2017, during the 28th Conference of the Heads of Governments of the Caribbean Community (CARICOM) held in Guyana. This document proposes a vision to promote a space without borders in the ICT field and the steps to follow for its establishment. This agreement is based on the work done by the Caribbean Telecommunications Union (CTU) through a series of documents and discussion meetings.[30] As part of this agreement, the countries approved an integrated work plan and a budget to promote the strategy. The plan details a set of research and communication activities, aimed at strengthening legal and regulatory convergence in telecommunications. The components of the plan are:[31]

i) Policies, legal and regulatory framework harmonized regionally on ICT.

ii) A strong national and regional broadband infrastructure.

[30] Subsequent discussions also included the Agency of the Caribbean Knowledge and Learning Network (CKLNA), the Caribbean Broadcasting Union (CBU), the CARICOM Crime and Security Agency (IMPACS), the Development Management Center of the Caribbean (CARICAD), and the CARICOM Secretariat.

[31] This plan is considered as the digital layer of the CARICOM Single Market and Economy (CSME).

iii) Common frameworks for governments, service providers, and consumers.

iv) Effective and safe technology and management systems.

The objective of the strategy is to provide enabling elements to facilitate the deployment of ICTs in the region, through the harmonization of regulatory and legal frameworks for the unfolding of broadband, information management systems, the provision of information technologies services, and improve the security of the digital space and management systems. This initiative is expected to promote a greater consistency in access, quality, and affordability of ICT services in the Caribbean community. The plan's deadline is 2019, and was created considering existing initiatives but with the possibility of escalating its scope (CTU, 2017).

E. The Pacific Alliance

The Pacific Alliance aims to benefit its population through the free movement of goods, services, capital, and people.[32] It considers that trade and integration are achieved by regulating provisions related to tariff liberalization, rules of origin, and technical barriers to trade, among others. To date, it has eliminated 92% of tariff rates among its four countries and has agreed to eliminate the remaining 8% in the coming years.

The Additional Protocol of the Framework Agreement of the Pacific Alliance includes a chapter on telecommunications and another on electronic commerce. The main measures in the telecommunications chapter addresses issues such as (Colombia, Chile, Peru, and Mexico, 2014):

- Non-discriminatory interconnection.
- Number portability.
- Equitable allocation and use of scarce resources.
- International roaming.
- Competitive safeguards, important to prevent dominant agents from developing anticompetitive practices and facilitating market entry; effective dispute resolution, and universal service.

The chapter on electronic commerce applies to electronic transactions of goods and services, including digital products, and aims to facilitate trade carried out by electronic means. Its main topics consider:

- Facilitation of electronic commerce, avoiding and eliminating unnecessary obstacles.
- Customs duties.
- Rules and procedures for advertising.
- Rules on consumer protection. Personal data protection.
- Authentication and digital certificates.
- Cross-border information flow.

The Innovation Group of the Pacific Alliance has a subgroup on the Digital Agenda (SGAD), created at the 11th Summit of the Pacific Alliance (Chile, July 2016). Its objective is to implement, develop and deepen specific topics included in the chapters of telecommunications and electronic commerce. It is specified that the SGAD can also address aspects of the eLAC2018 regional digital agenda adopted at the Fifth Ministerial Conference on the Information Society in Latin America and the Caribbean, held in Mexico City in 2015.

[32] The Pacific Alliance is a regional integration initiative formed by Chile, Colombia, Mexico, and Peru. It was officially created on 28 April 2011, and formally and legally constituted on 6 June 2012, with the signing of the Framework Agreement, which has an indefinite duration.

The first meeting of the SGAD took place in Santiago de Chile in December 2016. Its main result was the adoption of a roadmap within four pillars (digital connectivity, digital commerce, digital government, and digital ecosystem), for which specific objectives and actions were identified (Pacific Alliance, 2018).

An important aspect of the Pacific Alliance is that it was formed with the explicit purpose of establishing closer relations with the Asia-Pacific region. In the years prior to the establishment of the Pacific Alliance, its four-member countries had already begun to engage independently with their Asian peers (for example, Chile and Peru signed agreements with China, Singapore, and the Republic of Korea, Chile and Mexico negotiated free trade agreements with Japan, and Colombia signed an FTA agreement with the Republic of Korea). The alliance allows its members to formulate coherent trade policy decisions in search for business opportunities with Asian markets, including China.

Chile, Mexico, and Peru are members of APEC and participated in the negotiation of the TPP. Colombia is not a member of APEC or the TPP, but has tried to become a member of APEC since 1995 and has formally expressed interest in joining the TPP process. The Pacific Alliance could boost the incorporation of Colombia to the APEC group and, by extension, to the TPP.

The Pacific Alliance has made significant progress in trade integration, business facilitation, and coordinated diplomatic approaches. This has contributed to the progress of relations with Asian countries, while consolidating the image of its members.

In May 2017, the Pacific Alliance and the Association of the Southeast Asian Nations (ASEAN) renewed their commitment to strengthen cooperation between them at the 3rd meeting of the Committee of Permanent Representatives of ASEAN and the Alliance's Foreign Relations Group of the Pacific held in the ASEAN Secretariat. The parties reiterated the importance of deepening participation through the implementation of the ASEAN-Pacific Alliance Framework for Cooperation, approved at the 3rd Ministerial Meeting of the ASEAN-Pacific Alliance, held in New York in September 2016. The cooperation framework prioritizes four areas: economic cooperation; education and people engagement; science, technology and innovation; and sustainable development (ASEAN, 2017).

Finally, on 2 June 2017, the Pacific Alliance countries announced the definition of the requirements and associated procedures for the submission of applications to become member countries, a key element for its expansion (Pacific Alliance, 2017).

F. The Common Market of the South

The Mercosur was established in 1991, when Argentina, Brazil, Paraguay, and Uruguay signed the Treaty of Asunción, with the aim of creating a customs union and establishing a Common Market for the South with the objective to free the circulation of goods, capital, services, and people among its members. In 1994, it was institutionally restructured through the Protocol of Ouro Preto and became subject to international law. Although initially the block focused on economic and trade issues, in the last two decades regional integration was strengthened in the cultural, educational, structural, and productive areas (Mercosur, 1994).

Mercosur has six members and is open to incorporations, through negotiation, by members of the Latin American Integration Association (ALADI), an association that includes 13 countries of the region and dates back to 1980 (established by the Treaty of Montevideo).

The Treaty of Asunción provides a basic structure for Mercosur and the Protocol of Ouro Preto establishes a detailed institutional framework. The current structure is intergovernmental and not supranational, since there has been no transfer of sovereignty, a way in which Mercosur differs from the European Union and the Andean Community of Nations (CAN). In contrast, Mercosur has similarities with the EU regarding the goal to achieve the free movement of citizens and workers within the area. This feature of Mercosur is unique in the region and differs substantially from other associations.

Decisions are adopted by consensus of all member states and are binding. The member states must incorporate the decisions in their domestic legal system, with the exception of decisions related to procedures and the internal organization of Mercosur bodies, which are fully enforced (Mercosur, 2014).

The Common Market Group (CMG) of Mercosur operates through a structure that includes subgroups with tasks related to the identification of issues that must be harmonized. Among the subgroups is SGT 1, which covers communication services. In October 2015, SGT 1 proposed a work plan for the 2016-2017 period. SGT 1 has established four committees to support the work of CMG to reach a common telecommunications and postal services market. Its activities seek to eliminate the regulatory aspects that hinder the integration of that market and coordinate the positions adopted by Mercosur in international forums. Its committees are the Postal Affairs Commission (CTAP), the Broadcasting Committee (CTRd), the Radiocommunication Committee (CTRc) and the Public Telecommunications Services Committee (CTSPT) (URSEC, 2017).

Table 10
Telecommunications and broadcasting issues under the responsibility of SGT 1

Telecommunications	Media / broadcasting
Critical infrastructure	Information exchange on the evolution of digital terrestrial television
Fraud prevention systems	Coordination of stations (AM, FM and TV) with the consolidation of an information database
Telecommunications indicators	Interference and notification of operation of irregular stations
Numbering of resources in the different telecommunications services	
Neutrality of the network	
Users rights	
IP Interconnection (IXP)	
Digital mobile financial services	

Source: Communication Services Regulatory Unit (URSEC) (2017).

In 2010, Mercosur approved a Statute of Citizenship[33], which, among other purposes, aims to reduce international roaming tariffs for people traveling within the area, and have local pricing in the areas near the boarders. These measures should be applied before 2021. Currently, member countries are defining possible measures for pilot projects (Mercosur, 2017).

[33] Mercosur/CMC/DEC N° 32/17.

VI. Conclusions

In terms of IoT infrastructure it is important to encourage regulatory frameworks that promote efficiency in the allocation of the radio spectrum; new mobile connectivity technologies increasingly require spectrum use (both licensed and unlicensed). On the other hand, cross-border e-commerce requires the reduction of non-tariff trade costs and facilitate the flow of goods and services, since there are several issues related to paperless trade that require attention, in particular, the importance of the electronic single window for foreign trade (ESW) and the creation of the legal and technical conditions to facilitate the exchange of electronic data on trade between countries.

In relation to postal performance, policymakers must develop strategies to improve the operation of national postal services. This is one of the areas in which the region is lagging behind. On the matter of online payment, emphasis must be placed on the promotion of more flexible regulations to motivate innovation and digital financial inclusion, following international recommendations. In terms of consumer protection, it is important that countries update their regulations about digital commerce and also promote self-regulation mechanisms for the prevention of deceptive practices and conflict resolution. Cybersecurity is another area in which it is necessary to continue with regional cooperation efforts and national strategies, taking into account technical, organizational, and institutional aspects, and considering ongoing cooperation initiatives.

The coordinated and harmonized elimination of national barriers that hinder cross-border trade and investment in digital markets, combined with the coordination of the legal and regulatory frameworks throughout the region, could create significant economic and social benefits. Better regional organization and harmonization could lead to:

- Increased investor confidence and more foreign direct investment.
- Promote innovation and economic diversification.
- Promote cross-border trade and confidence in the use of electronic commerce and payments among more than 600 million consumers in the region.
- Strengthen demand for high quality connectivity.
- Increase productivity, particularly for small and micro enterprises.

Despite the lack of supranational authorities, greater regional coordination could be achieved through a regional digital integration plan that establishes:

- A common vision.
- Common priorities, objectives, goals, specific milestones, resources, governance, and a clear calendar.
- Conditional acceptance of deadlines, combined with systems of voluntary and gradual application of measures that recognize specific national circumstances, without delaying the general calendar.
- Effective coordination and financing mechanisms.
- Mechanisms for dialogue and coordination with existing subregional and regional organizations.
- Provision of adequate technical staff, clear leadership, and effective management of financial resources.
- Control and evaluation mechanisms to guarantee implementation.

Despite some good practices implemented in various countries, the digital economy in Latin America and the Caribbean lags behind compared with other areas in the world. Regardless of regional and sub-regional efforts, considerable fragmentation, duplication of activities, and inefficient coordination persist, resulting in a maze of legal and regulatory environments and the underutilization of resources (Cullen International, 2017). In this scenario, the formulation and implementation of a common strategy that progressively integrates legal and regulatory frameworks would boost investments in the digital economy, with its consequent positive effects on growth, productivity, and employment for the regional economy. Such a common strategy needs to complement existing economic integration agreements to advance.

Bibliography

ALADI (Latin American Integration Association) (2013). "Certificación de origen digital de la ALADI", Managua, ALADI.

Pacific Alliance (2018), "Grupos Técnicos, Agenda digital", [online], [date of consultation: March, 2017], https://alianzapacifico.net/grupos-tecnicos/.

Pacific Alliance (2017), "Consejo de Ministros de la Alianza del Pacífico firman lineamientos de la figura de Estado Asociado", [online], [date of consultation: March, 2017], https://alianzapacifico.net/con sejo-de-ministros-de-la-alianza-del-pacifico-firman-lineamientos-de-la-figura-de-estadoasociado-2/.

AliResearch (2014), "Global Cross Border B2C Ecommerce Market 2020", AliResearch.

Asia-Pacific Economic Cooperation (APEC) (1998), "APEC Blueprint for Action on Electronic Commerce", [online], Santiago de Chile, [date of consultation: March, 2017], http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan012805.pdf.

Asia-Pacific Economic Cooperation (APEC) (2014), "Connectivity Blueprint for 2015-2025", [online], [date of consultation: March, 2017], https://www.apec.org/Meeting-Papers/Leaders-Declarations/2014/2014aelm/2014_aelm_annexd.

Asia-Pacific Economic Cooperation (APEC) (2015a), "APEC Telecommunications and Information Working Group Strategic Action Plan 2016-2020", [online], [date of consultation: March, 2017], https://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information.

Asia-Pacific Economic Cooperation (APEC) (2015b), "APEC Privacy Framework", CTI Sub-Fora & Industry Dialogues Groups, Electronic Commerce Steering Group (ECSG), August 2017.

Association of Southeast Asian Nations (ASEAN) (2017), "ASEAN, Pacific Alliance to strengthen cooperation", [online], [date of consultation: March, 2017], http://asean.org/asean-pacific-alliance-to-strengthen-cooperation/.

Inter-American Development Bank (BID) (&) Finnovista. (2017), "Fintech – Innovaciones que no sabías que eran de América Latina y el Caribe", [online], [date of consultation: March, 2017], https://publications.iadb.org/bitstream/handle/11319/8265/ FINTECH-Innovaciones-que-no-sabias-que-eran-de-America-Latina-yCaribe.pdf?sequence=2&is Allowed=y.

Bazot, G. (2013), "Financial consumption and the cost of finance: Measuring financial efficiency in Europe (1950-2007)", Working Paper Paris School of Economics.

BBC (2017, "13 May), "Cyber-attack: Europol says it was unprecedented in scale", [online], [date of consultation: July 2017], http://www.bbc.com/news/world-europe-39907965.

CARICOM (2017), "CARICOM Today, Agencies meet after Heads of Government approve Single ICT Space Roadmap", [online], [date of consultation: July 2017], http://today.caricom.org/2017/02/27/agencies-meet-after-heads-of-government-approve-single-ict-space-roadmap/.

European Union (2017), "EUR-Lex. Access to European Union Law. Revised rules for payment services in the EU", [online], [date of consultation: February 2017], http://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32015L2366.

El Salvador, Ministerio de Relaciones Exteriores y Proyecto Integración y Desarrollo Mesoamérica, (2013), *Lineamientos Estratégicos y Plan de Acción para la Agenda Mesoamericana de Integración de los Servicios de Telecomunicaciones (AMIST)*, San Salvador, January.

El Salvador, Guatemala, Honduras and Nicaragua (1993), *Protocolo al Tratado General de Integración Económica Centroamericana (Protocolo De Guatemala)*, Managua, December.

Colombia, Chile, Perú and Mexico (2014), *Protocolo Adicional al Acuerdo Marco de la Alianza del Pacífico*, Cartagena de Indias, February.

CEPAL (2016), *Panorama de la Inserción Internacional de América Latina y el Caribe: La región frente a las tensiones de globalización*, (LC.G.2697-P), Santiago de Chile: United Nations.

CEPAL (2015). *Encuesta Global sobre Facilitación e Implementación del Comercio sin Papeles, Resultados para América Latina y el Caribe*. Santiago de Chile: United Nations.

CNN Tech (2017), "Massive malware attack: Who's been hit", [online], [date of consultation: July 2017], http://money.cnn.com/2017/06/28/technology/ransomware-attack-whos-been-hit/index.html.

Cullen Intenational (2018), "Regional and Subregional Approaches to the Digital Economy: Lessons from Asia-Pacific and Latin America", study prepared by Cullen International for CAF – Development Bank of Latin America, unpublished.

Caribbean Telecommunications Union (CTU) (2017), "Vision and Roadmap for a CARICOM Single ICT Space", approved at the Twenty-Eighth (28th) Inter-Sessional Meeting of the Conference of Heads of Government of the Caribbean Community (CARICOM) Georgetown, February.

Consumer Barometer (2015), "Consumer Barometer with Google", [online], [date of consultation: April 2017], https://www.consumerbarometer.com: https://www.consumerbarometer.com.

eMarketer (2015), "Worldwide Retail Ecommerce Sales: Emarketer's Updated Estimates and Forecast", Market research company.

Financial Stability Board (FSB) (2017), "Financial Stability Implications from Fintech" [online], [date of consultation: February 2017], http://www.fsb.org/wp-content/uploads/R270617.pdf.

Google (2015), "Consumer Barometer Survey", [online], [date of consultation: January 2017], https://www.consumerbarometer.com/en/.

GPFI (2014), "Digital Financial Inclusion and the Implications for Customers, Regulators, Supervisors and Standard-Setting", 2nd GPFI Conference on Standard-Setting Bodies and Financial Inclusion: Standard Setting in the Changing Landscape of Digital Financial Inclusion, Global Partnership for Financial Inclusion.

International Telecomunications Union (ITU) (2017). *Global Cybersecurity Index*. Geneva: United Nations.

International Telecomunications Union (ITU) (2017), "World Telecommunication/ICT Indicators database 2017", [online database], [Accessed August 2017].

Lachowicz, M. S. (2016). "Pagos Móviles en América Latina y el Caribe", [online], [date of consultation: July 2017], http://oif.ccee.edu.uy/wp-content/uploads/2016/01/pagos_moviles_en_america_latina_y_el_caribe-enero_2016_0.pdf.

Mercosur (1994), *Protocolo Adicional al Tratado de Asunción sobre la Estructura Institucional del Mercosur -Protocolo de Ouro Preto-*, Ouro Preto.

Mercosur (2014), XLVII Reunión Ordinaria del Consejo del Mercado Común, Paraná, December.

Mercosur (2017), *Estatuto de la Ciudadanía del Mercosur Plan de Acción Actualización de la Decisión CMC N 64/10*, Brasilia, December.

Malstrom, C. (2016), *Trade in a Digital World*, Discurso en la Conferencia de Comercio Digital del Parlamento Europeo, November, Brussels [online], [date of consultation: July 2017], http://trade.ec.europa.eu /doclib/docs/2016/ november/tradoc_155094.pdf.

Martens, B. (2013). "What does Economic Research tell us about Cross-border e-Commerce in the EU Digital Single Market? A Summary of Recent Research", Luxembourg: European Union.

McKinsey & Company (2015), "Global Payments 2015: A Healthy Industry Confronts Disruption", McKinsey & Company.

McKinsey Global Institute (MGI) (2016), "Digital Globalization: The New Era of Global Flows", [online], [date of consultation: July 2017], http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalizationth e-new-era-of-global-flows.

Nielsen Newswire (2015), "Preferred payment methods of online shoppers in Latin America as of 4th quarter 2015". [online], [date of consultation: April 2017], https://www.statista.com/statistics/256262/ preferred-payment-methods-of-online-shoppers-in-latin-america/.

Omar, D. (2017), "Apoyo a la implementación del Programa Estratégico de Especialización de Industrias Inteligentes", documento preparado para el proyecto Convenio de Colaboración CEPAL y CORFO, Santiago de Chile, inédito.

OECD (2017), *Key Issues for Digital Transformation in the G20*. París: OECD.

OECD (2014), *Consumer Policy Guidance on Intangible Digital Content Products*. Paris: OECD.

OECD & WTO (2017), Aid for Trade at a Glance 2017: Promoting Trade, Inclusiveness and Connectivity for Sustainable Development, WTO, OECD Publishing, Geneva.

Philippon, T. (2015), "Has the US finance industry become less efficient? On the theory and measurement of financial intermediation", The American Economic Review, 105(4), 1408–38.

Salido J., (2015), "Una mirada a los países del Proyecto Mesoamérica", Document prepared for the XV Summit: *Cumbre del Mecanismo de Diálogo y Concertación de Tuxtla Ciudad de Guatemala*, Guatemala Friday 26 June 2015, (LC/MEX/L.1183), United Nations, Mexico, D.F.

Sistema de la Integración Centroamericana (SICA) (2015), "Estrategia Regional Digital del SICA", Secretaría General del Sistema de la Integración Centroamericana, March.

UNCITRAL (2017), Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales, [online], [date of consultation: July 2017], http://www.uncitral.org/ uncitral/uncitral_texts/electronic_commerce/2005Convention.html: http://www.uncitral.org/uncitral/unci traltexts/electr onic_commerce/2005Convention.html.

United Nations Conference on Trade and Development (UNCTAD) (2017), *E-trade indicators*, Geneva: United Nations.

United Nations Conference on Trade and Development (UNCTAD) (2017), *B2C E-commerce Index*, Geneva: United Nations.

United Nations Conference on Trade and Development (UNCTAD) (2016b), *Examen de la armonización de la ciberlegislación*, Geneva: United Nations.

United Nations Conference on Trade and Development (UNCTAD) (2016b), *Directrices para la Protección al Consumidor*, Geneva: United Nations.

United Nations Conference on Trade and Development (UNCTAD) (2015), *In search of cross-border e-commerce trade data*, Geneva: United Nations.

United Nations Regional Commissions (2015), "Trade Facilitation and Paperless Trade Implementation Survey, Latin America and the Caribbean Report", Santiago de Chile: United Nations.

Universal Postal Union (2016), "Integrated Index for Postal Development (2IPD)", Bern: Universal Postal Union.

USTR (Oficina del Representante Comercial de los Estados Unidos) (2016), "The Digital 2 Dozen", Washington, D.C., [online], [date of consultation: July 2017], https://ustr.gov/sites/default/files/Digital-2-Dozen-Final.pdf.

Unidad Reguladora de Servicios de Comunicación (URSEC) (2017), *Mercosur Información General*, [online], [date of consultation: July 2017], https://www.ursec.gub.uy/inicio/institucional/institucional-relaciones-internacionales/relacio nes-internacionales-mercosur/.

World Bank (2016), "FinTech and Financial Inclusion", [online], [date of consultation: June 2017], from http://pubdocs. worldbank.org: http://pubdocs.worldbank.org/en/877721478111918039/breakout-DigiFinance-Mc Conaghy - Fintech.pdf.

World Bank (2014), "Global Finance Inclusion Database". [online], [date of consultation: July 2017], http://www.worldbank.org/ en/programs/globalfindex.

Annex

Digital provisions in regional integration agreements

	APEC	SICA	Mesoamerica	Pacific Alliance	MERCOSUR	TPP
Regional Agenda	Telecommunications Action Plan 2016-2020. Policy Partnership on Science, Technology and Innovation *(PPSTI), 2016-2025*.	*Digital strategy (proposal of 2015).*	Mesoamerican Agenda for the Integration of Telecommunications Services (AMIST) and a related action plan were discussed in 2013, but were not implemented.	*Road Map (approved in 2016).*	Action Plan for Citizenship Statute (CMC-64/10) SGT 1 programme (2016-2017*).*	An agenda does not exist. Principles on digital economy in the TPP (2016).
Connectivity	Pilot projects and exchange of information on rural connectivity / NGN / Accessibility.	Promote universal access to broadband.	Project REDCA.	Create infrastructure to develop IXP. Promote investment, public-private partnership. Evaluate joint actions. Encourage net neutrality adoption.	Analysis and exchange of information on the convergence of networks and services. Impact studies on application networks and OTT services. Survey, monitoring, and exchange of information regarding tariffs, prices, and taxes on telecommunications services, reference cost models (regulatory accounting), and interconnection.	Network neutrality, principles of free and open internet. Robust regulatory frameworks that promote investment.
Digital literacy	Education projects Exchange of policy information.	ICT use for inclusive education. Promote digital skills.			Mercosur Digital - training for MSMEs.	
International roaming fee	Explores principles and possible measures.			Dialogue to promote transparency and competition in the market. Identify international cooperation strategies.	Reduce international roaming rates among members. Eliminate charges for roaming in border areas, through the use of shared networks.	Reduce international roaming fees among members, promote competition in the market.
Standards and interoperability .	Technical compliance assessments. Equivalence of technical requirements.			Adoption of the IPv6 standard in the public sector. Exchange of best practices and horizontal cooperation in interoperability and digitalisation.	Analysis and exchange of information on: National numbering plans. Mapping of telephone number, ENUM. Transition to IPv6. Consider possible measures.	Transparent and non-discriminatory rules for the development of standards and technical regulations. The parties agree to cooperate to ensure that technical regulations and standards do not create unnecessary obstacles to trade.
ICT adoption	ICT applications (banking, health, government). Entrepreneurship MIPYMES.	Promote the use of ICT to: Government services for citizens. Environment Social Security.		Exchange of best practices and experiences of horizontal cooperation, administrative simplification, reduction of the gaps in digital adoption. Regional Observatory of digital government.		

	APEC	SICA	Mesoamerica	Pacific Alliance	MERCOSUR	TPP
Cybersecurity	Cybersecurity framework. Several projects.					Help build cybersecurity capacities to prevent cyber attacks and malware distribution.
Innovation / R&D	IoT. app2app. Strategic science, technology and innovation policy plan (PPSTI). Smart cities. Artificial intelligence. Nanotechnologies.	Promote R&D throughout the region, close gaps between large companies and MSMEs. Promote technology transfer		Encourage technical cooperation in the use of shared services, cloud computing, hardware security module (HSM), electronic signature, among others.	Exchange experiences in R&D.	Investment and cross-border service commitments, allowing providers to offer cloud computing and other technology services in all TPP countries.
Institutional and regulatory environment	Analyse / exchange information on policies, competition and barriers to trade. Statistical evaluations Paperless trade, use of digital customs forms.	Promote inter-institutional coordination through the use of ICT.	Promote dialogue within the Mesoamerican Forum of Telecommunications Authorities (FMAT). The FMAT has not been institutionalized.	Implement a regional digital market, taking as reference the regional eLAC agenda. Study joint measures that allow investment in high-speed networks (competition, sectoral regulation, elimination of obstacles).	Establish harmonized indicators of the telecommunications market. Exchange of information and analysis on the possible harmonization of: The broadband and telecommunications plans. Parameters on service quality. Prevention of fraud. Internet of things. Network neutrality. User rights. Other standards Evaluation of possible measures that should be taken.	Regulation of telecommunications networks (harmonize the frameworks on key aspects). Maintain legal regimes that prohibit anti-competitive practices and fraudulent and deceptive commercial activities. Total prohibition of customs duties for digital goods and services. Commitments on the facilitation of customs and trade procedures, including paperless trade, using digital customs forms.
E-commerce	Platforms, support to MIPYMES, electronic payment projects, external collaboration.			Information and cooperation in the field of digital identifiers, digital signatures.	Digital Mercosur, promotion of electronic commerce.	Adopt and maintain applicable consumer protection standards (including privacy) to provide a reliable environment for electronic commerce. No technological barriers to the selection of technology and encryption solutions (including digital signature and electronic payment solutions).
Promotion of digital content / applications		Explicit reference to the UN Declaration on Freedom of Expression.		Facilitate the use of public software, through the existing platform.		
Privacy and data	APEC's Privacy Framework. Arrangement on Transboundary Privacy Application. Transboundary Privacy Rules System. APEC-EU working committee.			Implementation of the International Charter on Open Data. Technical cooperation between countries: diagnostics.		Access to networks and efficient data processing, including not requiring TPP companies to build data centers to store data as a condition of operating in a TPP market. The transfer or access to the source code of the software is not required.

	APEC	SICA	Mesoamerica	Pacific Alliance	MERCOSUR	TPP
Intellectual Property						Copyrights, patents, trademarks, industrial designs, norms on the obligation of companies to transfer their technology or production process. Systems of enforcement / establishment of criminal procedures and criminal sanctions.

Source: Cullen International (2018), "Regional and Sub regional Approaches to the Digital Economy: Lessons from Asia-Pacific and Latin America", document prepared by Cullen International for CAF - Development Bank of Latin America, unpublished.

The digitalization of economies is being driven strongly by the incorporation of advanced technologies at all the links of the productive process of different industries.

This has resulted in a reconfiguration of the world economy and in larger gaps between the countries that lead these processes and those that have yet to develop the capacities to compete in an increasingly digital world.

In this new global economic context, our region faces several important challenges, including the need to develop appropriate infrastructure that supports innovation, as well as the possibility of creating a regional digital market that will allow the countries of Latin America and the Caribbean to face this scenario from the perspective of regional integration.

This document identifies certain barriers and obstacles to the expansion of the digital economy in the region, proposes some strategic lines of action and presents a set of objectives aimed at guiding policy decisions regarding connectivity, electronic commerce, postal performance, consumer protection, digital financial inclusion and online means of payment and cybersecurity, in addition to reviewing chapters pertaining digital matters of regional economic integration agreements.

ECLAC

Economic Commission for Latin America and the Caribbean (ECLAC)
Comisión Económica para América Latina y el Caribe (CEPAL)
www.eclac.org