BUILDING A DIGITAL SINGLE MARKET STRATEGY FOR LATIN AMERICA

CAF DEVELOPMENT BANK OF LATIN AMERICA

BUILDING A DIGITAL SINGLE MARKET STRATEGY FOR LATIN AMERICA

Title
Building a Digital Single Market strategy for Latin America

Editor
CAF
Corporate Vicepresident, Infraestructure Antonio Juan Sosa
Telecommunications and Digital Economics Specialist and Coordinator of this study, Mauricio Agudelo

Author
Cullen International

Graphic design
Estudio Bilder / Buenos Aires

Cover photo
Ilya Pavlov

The digital version of this book is available at: scioteca.caf.com

CONTENTS

FIGURES

EXAMPLES

TABLES

EXECUTIVE SUMMARY

This report, prepared by Cullen International on behalf of CAF – Development Bank of Latin America, aims to identify and discuss the possible scope, opportunities, and main legal and regulatory challenges associated with the launch of a Digital Single Market (DSM) strategy in Latin America.

As is known, the DSM strategy is the European Commission's overarching vision on digital issues for 2015-2020. It includes the Commission's priorities for the review of the EU regulatory framework for electronic communications, as well as a number of legislative reviews and other actions, aiming to *"... make the EU's single market fit for the digital age —tearing down regulatory walls and moving from 28 national markets to a single one. This could contribute €415 billion per year to our economy and create hundreds of thousands of new jobs"*[1].

The EU and Latin America each have a population of approximately 500 million. The perspective of building a 'single market' of 500 million consumers is particularly attractive in economic terms.

There is a conceptual challenge in comparing the EU's existing single market with a potential, prospective Latin American single market.

To a European, 'single market' means a decades-long path of economic, social and political integration, based on the EU Treaties and implemented and enforced by a common set of laws, institutions, and rules.

Latin America —in contrast to the EU— is a group of individual nations within a single, very large geographic region. These countries often share similar cultural identities and language, but are still lagging behind in exploiting the full potential of a more intense regional trade, or in establishing more integrated economic and social development policies.

The idea of building a DSM for Latin America could be considered as particularly challenging and ambitious, given the lack of a Pan-American institutional framework with binding powers over Latin American countries.

In the EU, where national barriers leading to a 'single market' for goods and services have been removed in the physical world, considerable challenges still exist when we consider digital markets.

In the words of the 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."[2]

In this document we investigate whether there is room for development of a DSM for Latin America. As is known, no single market or trade area has ever been created for the whole Latin American region.

Would a more integrated and consistent regional approach for digital policies and regulations across Latin America increase the economic and social development opportunities linked to the digital age?

What level of policy and regulatory integration would be desirable? What barriers should be removed to make a DSM for Latin America possible?

The EU DSM strategy is built upon three pillars:

1. better access for consumers and businesses to online goods and services across Europe;

2. creating the right conditions for digital networks and services to flourish; and

3. maximising the growth potential of the European digital economy.

This report is divided into two parts.

In the first part, we briefly present the rationale, objectives and proposals of the EU Commission's digital single market strategy. A brief description of the most relevant DSM-related policy and regulatory issues will be presented, from an EU perspective.

Our analysis is mainly focused on the first two pillars of the EU DSM strategy:

— creating the right conditions for digital networks and services to flourish (including fostering network infrastructure investment and services take-up, spectrum harmonisation, and standardisation policies); and

— better access for consumers and businesses to online goods and services across Europe (including e-commerce and new digital economy regulatory debates such as those on cloud computing, and the sharing economy).

In the second part of the report we present the same topics, but from a Latin American perspective. In particular, we discuss whether and how individual Latin American countries have been addressing the policy or regulatory issues currently discussed in the EU under the DSM strategy, and whether any regional initiative has been launched or proposed to remove certain existing legal or regulatory barriers across Latin America on such issues.

In the final part of this report we discuss the current involvement of regional and sub-regional organisations in specific debates or initiatives for each of the topics analysed. We will also summarise the main findings, and indicate the main obstacles for the creation of a flourishing digital single market in Latin America.

The DSM-related key initiatives analysed in the report, from the EU and the Latin American perspectives, are summarised in Table 1 below, which also indicates the relevant regional or sub-regional entities involved.

TABLE 1
Summary of main DSM-related goals in the EU and Latin America (Cullen International)

	Europe		Latin America	
	key initiatives	**by whom**	**key initiatives**	**by whom**
		Better connectivity		
BB coverage and take up	EU Digital Agenda National BB plans	EU Commission National governments	National BB plans	National governments Technical assistance initiatives by multilateral org.)
Rural divides	State aid guidelines Connecting Europe facility	EU Commission EU Commission / EIB	Plans and projects at national level	National governments Technical assistance initiatives by multilateral org.)
Regional backbone networks	None. Trans-European networks (TEN) concern other sectors	Not applicable	Infrastructure in South America Submarine cables Initiatives at national level (large countries)	UNASUR/Cosiplan Multilateral agreements between public and private entities (governments, operators, fin. inst.)
Net neutrality	Part of the Telecom Single Market (TSM) Regulation (directly enforced in Member States)	EU Commission EU Parliament and Council	Studies and sharing of information Laws and implementing regulations at national level	Regulatel
International roaming	Part of the Telecom Single Market (TSM) Regulation (directly enforced in Member States)	EU Commission EU Parliament and Council	Studies and sharing of information Industry-led initiatives	Regulatel Multilateral organisations, IADB GSMA
Pro-invest. regulatory reform	Review of the EU regulatory framework	EU Commission BEREC Industry associations	Plans (if any) at national level	National governments and regulators
Spectrum harmonisation and standardisation	Ongoing activities Proposals on more EU coordination at technical level might be expected	RSPG CEPS EU Commission and RSC	Coordination in view of WRCs All relevant decisions are still at national level	ITU/regional entities and CITEL Regulatel
IP interconnection and IXPs	No relevant bottlenecks	Not applicable	Studies and monitoring Academic networks (e.g. RedCLARA)	Academic and research Internet domain names nat. institutions Regulatel
Interoperability (incl. new business models, OTTs)	Debate on within the Review	EU Commission BEREC Industry associations	Nascent debate, only in a few countries	Industry associations
		Boosting e-Commerce and improving online consumer experience		
Online contracts	Draft Regulation on addressing geo-blocking. Draft Directive to harmonise online consumer contracts. Draft Directive on the supply contracts of digital content. Draft Directive on cooperation between national consumer protection authorities. Platform on online dispute resolution.	EU Commission, Parliament and Council	Guidelines and draft model law on electronic transferable records Online dispute resolution Resolution N. 21/2004 on transparency guidelines	UNCITRAL Mercosur

Continued on next page →

	Europe		Latin America	
	key initiatives	**by whom**	**key initiatives**	**by whom**
Digital signatures	eIDAS Regulation of July 2016, replacing old e-signature rules	EU Commission, Parliament and Council	Plan on digital certification Studies, identity management Initiatives on e-trust	Mercosur TPP UNCITRAL
e-Payments	Payment Services Directive, 2015 Development of open technical standards	EU Commission, Parliament and Council European Banking Authority (EBA	Studies on mobile payments Industry studies	UNCITRAL GSMA
Taxation	Legislative proposals to modernise and simplify VAT for cross-border e-commerce Review VAT Directive, for treatment of e-books	EU Commission, Parliament and Council	Sub-regional customs agreements and recommendations Studies on the taxation of digital services	Aladi, FTA-Alca, Alianza del Pacifico, Caricom, Comunidad Andina, Mercosur CAF, ECLAC and Cet.la, GSMA, IIRSA and Regulatel
Copyright and piracy	Copyright Action Plan Copyright package Review of IPRED Directive Review of liabilities on online platforms: under consideration	EU Commission	No regional initiatives on copyright Alianza, to help fight online piracy	Alianza (industry initiative)
Privacy and data protection	New General Data Protection Regulation (GDPR) Review of safe harbour	EU Commission, Parliament and Council	Legislative guidelines 2015 Included in eLAC 2018 Several initiatives at national level	OAS ECLAC and governments
Cybersecurity	Network and Information Security (NIS) Directive Initiatives and projects at EU level	EU Commission, Parliament and Council ENISA European Cybercrime Centre (EC3) within Europol	International cooperation on sharing of information, forums of debate	Unasur, Mercosur, ICANN, ITU, OAS and the FIRST (Forum of Incident Response and Security Teams)
	New services and business models			
Big data	Free flow of data initiative	EU Commission	No regional or sub-regional initiatives	Not applicable
IoT	Free flow of data initiative Open standards Regulatory treatment	EU Commission EU Commission and BEREC within the Review	No regional or sub-regional initiatives	Not applicable
Cloud services	European Cloud strategy European Cloud initiative	EU Commission	No regional or sub-regional initiatives	Not applicable
Sharing economy	Communication Monitoring but no legislative or regulatory proposals	EU Commission	No regional or sub-regional initiatives	Not applicable

About Cullen International

Based in Brussels, for the last 30 years Cullen International has been monitoring, analysing, and reporting on the regulatory and policy developments for Telecommunications, Media, and, more recently also the Digital Economy and Postal sectors. Services covering Latin America's telecommunications and media were launched in 2010 and 2013 respectively.

For information about this report, please contact elena.scaramuzzi@cullen-international.com

PART I — EUROPE

1 —
UNDERSTANDING THE DSM STRATEGY IN THE EU INSTITUTIONAL CONTEXT

The EU is an economic and political union whereby its Member States[3] confer competences to attain a number of objectives[4], including the establishment of an internal market[5].

EU legislation is proposed by the European Commission, which promotes the general interest of the EU and takes initiatives to that end[6].

Both the European Parliament and the Council adopt legislation[7], normally in accordance with the ordinary legislative procedure (i.e. joint adoption by the two institutions (codecision)[8].

The European Parliament is composed of members directly elected by citizens of the 28 EU Member States, whereas the Council is composed of representatives from the governments of the 28 EU Member States.

The main legal acts that the EU can adopt are the following:

— Regulations, which are directly applicable in all Member States.

— Directives, which require that Member States adopt national implementing measures.

The internal market is one of the areas in which the Member States and the EU have a shared competence. This implies that both the EU and its Member States may legislate in that area. However, Member States may exercise their competences to the extent that the EU has not exercised them[9].

According to the Treaty on the Functioning of the European Union (TFEU), the internal market must constitute an area without borders in which the free movement of goods, persons, services and capital is ensured[10].

The EU is confronted with the situation that barriers that have been taken down in the physical market still remain in its digital sphere, due to the existence of different national on-line markets. The European Commission has already moved to put an end to this situation, launching in 2010 its Digital Agenda for Europe[11].

The European Agenda contained regulatory and non-regulatory actions that aimed at achieving by 2015 a number of 'key performance targets'[12], including:

— 50% of the population buying online by 2015;

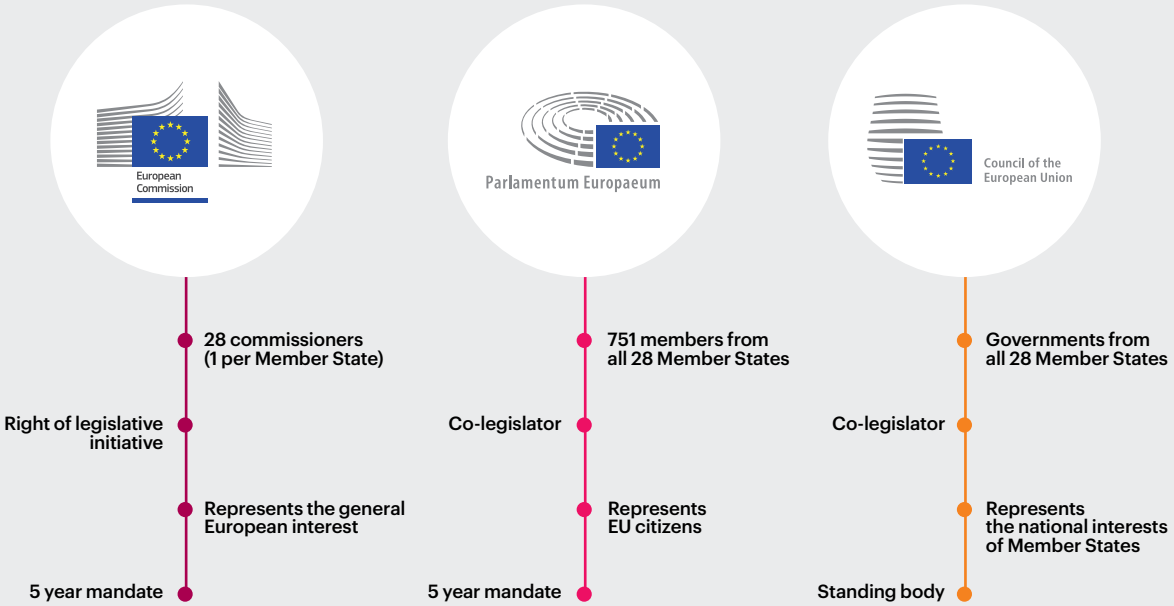
— 20% of the population buying cross-border online by 2015;

— 33% of SMEs conducting online purchases/sales by 2015.

TABLE 2
Digital Single Market Strategy for Europe

Better access for consumers and businesses to online goods and services across Europe	Creating the right conditions for digital networks and services to flourish	Maximising the growth potential of the European Digital Economy
e-Commerce rules	Telecoms regulatory framework	Interoperability and standardisation
Enforcement of consumer rules	Audiovisual Media Services rules	Big data, cloud, the Internet of Things
Cross-border parcel delivery	Online platforms and intermediaries	e-Government
Geo-blocking	e-Privacy rules	
e-Commerce sector enquiry	Cybersecurity	
Copyright reform		
Satellite and cable rules		
VAT		

FIGURE 1
EU institutional framework (Cullen International)



Some years later, these targets were far from being accomplished (for instance, only 17%[13] of SMEs in the EU sell online and only 7%[14] sell across borders, to other EU Member States) and regulatory barriers remain.

In this context, the Commission launched on May 6, 2015 its Digital Single Market Strategy for Europe[15]. The strategy is composed of 16 actions covering different topics and integrated into three pillars:

Most of these topics are addressed in the next chapters, together with other initiatives (e.g. online payments) that are not part of the Digital Single Market Strategy, but that were addressed in the past, as part of the Digital Agenda, and are relevant for the development of the Digital Single Market.

2 —
REGULATORY AND POLICY CONDITIONS FOR DIGITAL NETWORKS AND SERVICES TO FLOURISH

INFRASTRUCTURE AND DIGITAL SERVICES DEVELOPMENT ACROSS THE EU

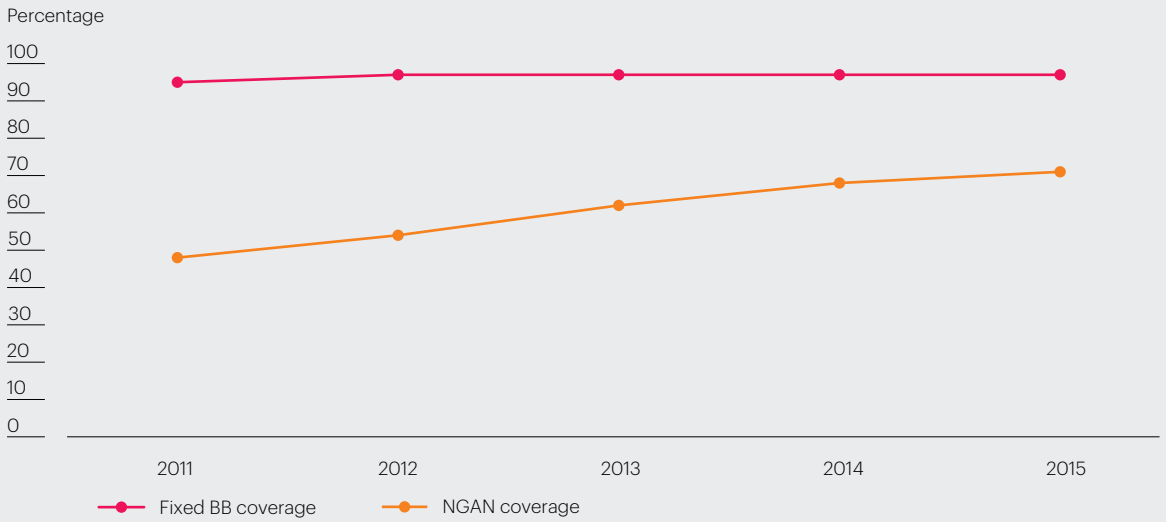
In the European Commission's perspective, the right conditions for digital networks and services to flourish can be identified with *"well-functioning markets that can deliver access to high-performance fixed and wireless broadband infrastructure at affordable prices. In this regard, the EU's telecoms rules aim to ensure that markets operate more competitively and bring lower prices and better quality of service to consumers and businesses, while ensuring the right regulatory conditions for innovation, investment, fair competition and a level playing field"*.

Opening telecommunications markets to competition was considered crucial for increasing the sector's efficiency, lowering prices and better serving consumers. In 1987, the European Commission issued a Green Paper in which it proposed the introduction of more competition in the telecommunications market, combined with a higher degree of harmonisation in order to maximise the opportunities offered by a single EC market, for example through economies of scale. This was the first step in a ten-year process which culminated in the liberalisation of all telecommunications services and networks from 1 January 1998.

The liberalisation process in the EU has been a particularly complex exercise, especially when compared with individual countries in the rest of the world. A set of binding rules had to be adopted at EU level prior to mandating their implementation in each EU Member State[16]. EU laws had to be transposed into national laws and enforced by independent national authorities, in accordance with the subsidiarity principle[17]. Non-compliance by Member States implied the possibility of opening EU infringement proceedings at the EU Court of Justice, something that occurred in practice on several occasions in the electronic communications sector[18].

Successive adaptations of the European telecoms framework, combined with the application of competition rules, have been instrumental in ensuring considerable progress in the sector across the EU. The impact of electronic communications networks and services' liberalisation has been regularly monitored by the EU Commission in its annual Implementation Reports[19].

FIGURE 2
EU average fixed broadband coverage (Cullen International based on EC data) a/



a/ 19th Implementation Report, 2015 https://ec.europa.eu/digital-single-market/en/news/implementation-eu-regulatory-framework-electronic-communications-2015 and European Commission - Connectivity: broadband market developments in the EU, 2015. https://ec.europa.eu/digital-single-market/en/connectivity Includes FTTP, VDSL and DOCSIS 3.0 coverage and Broadband Market Development in the EU 2016 https://ec.europa.eu/digital-single-market/en/connectivity

A STRONG FOCUS ON BROADBAND

In recent years most of the Implementation Reports' focus has been dedicated to the development of broadband networks and services and to the policies and regulatory conditions fostering their development and use.

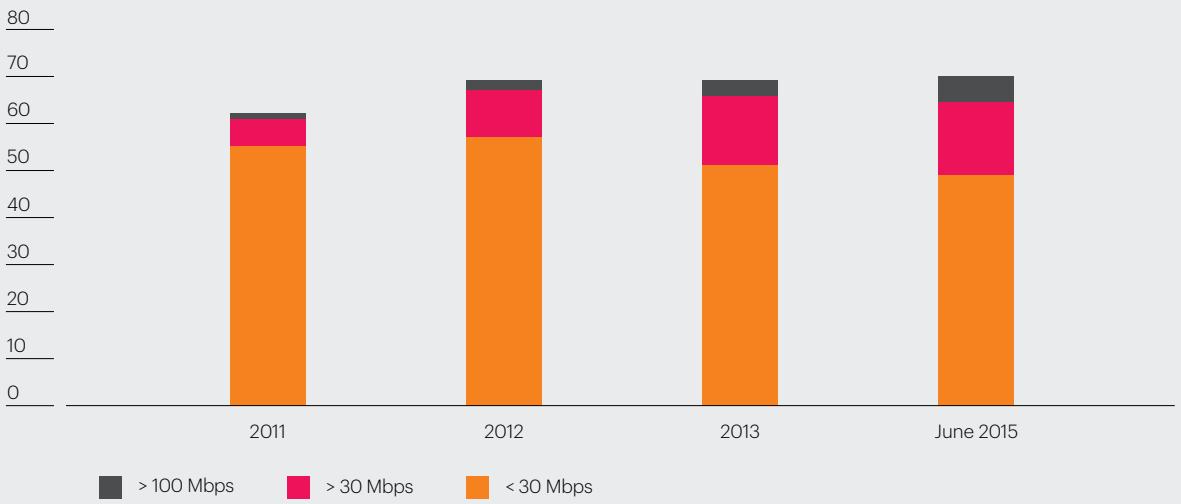
Broadband is notably considered an essential driver for growth, investment and innovation across the EU, and an essential element for the accomplishment of a single digital market, and the regulatory framework has been a significant enabler of increasing coverage, speeds and take-up of broadband.

> ***"All activities in the digital economy depend on electronic communication (broadband) networks. The DSM can only be realised when all European citizens, businesses and public administrations are connected to reliable, high-speed and affordable networks..."***[20].

Over the past few years, although fixed broadband network coverage has stabilised at an average of 97% of EU homes, take-up has increased from 62% of EU homes in 2011 to 71% in 2015. Coverage and take-up of next generation access networks (NGAN) show a more dynamic growth pattern, as is shown in the two figures below.

FIGURE 3

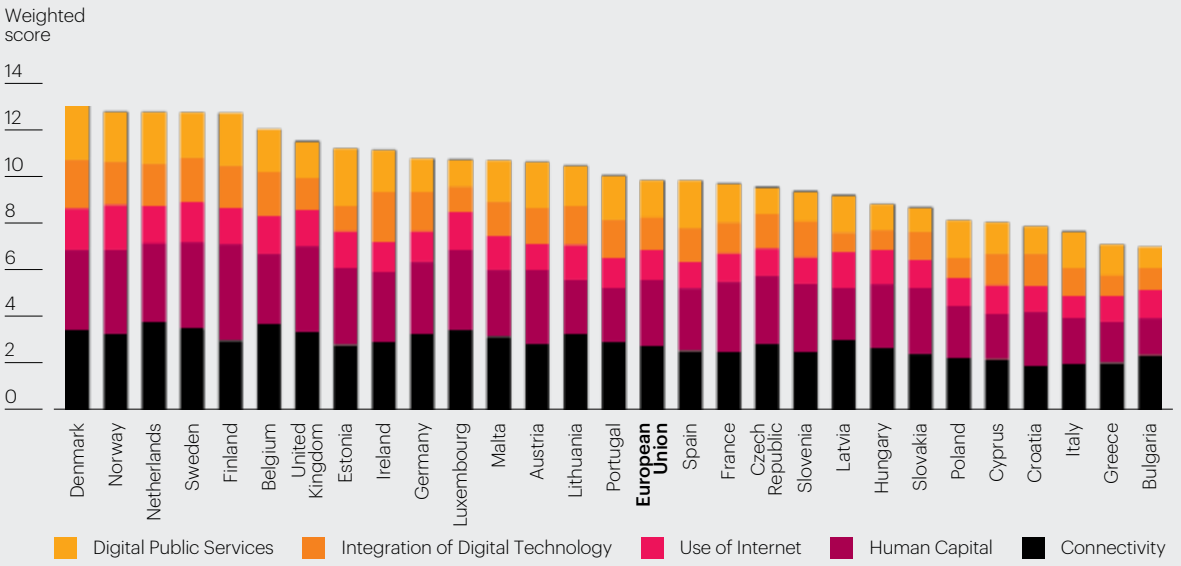
EU average fixed broadband take-up and speeds as a percentage of EU households (Cullen International based on EC data) [a/]



a/ 19th Implementation Report, 2015 https://ec.europa.eu/digital-single-market/en/news/implementation-eu-regulatory-framework-electronic-communications-2015 and European Commission - Connectivity: broadband market developments in the EU, 2015. https://ec.europa.eu/digital-single-market/en/connectivity Includes FTTP, VDSL and DOCSIS 3.0 coverage and Broadband Market Development in the EU 2016 https://ec.europa.eu/digital-single-market/en/connectivity

FIGURE 4

2016 Digital Economy and Society Index (European Commission)



As of October 2015[21], coverage of fast broadband technologies had reached 71% of homes, from 68% at end-2014. However, only 22% of European homes subscribed to fast broadband access of at least 30 Mbps and 8% subscribed to ultrafast broadband (at least 100 Mbps).

Fixed broadband coverage, penetration and technologies vary considerably across EU Member States. Over time, and even taking into account country specificities, we can say the EU regulatory framework has been quite successful in creating the conditions for effective competition in the distinct national markets. Traditional providers of vertically integrated telecoms services (incumbents) compete against access seekers (entrants) and with providers of cable networks (historically delivering television services). Incumbents' market shares in fixed broadband averaged 40% in the EU in June 2015[22].

Innovation in mobile broadband networks has also been significant in recent years. Alongside mobile broadband coverage (HSPA) that has been stable for years on average at 97%, Long Term Evolution (LTE) coverage grew on average from 8% in 2011 to 86% of the EU population as of October 2015. However, only 36% of rural areas were covered, and with very wide differences between Member States.

Mobile broadband service subscribers grew from 2011 to 2015 from 47% to 78% of the EU population[23].

LTE networks have been launched commercially in almost every European country. The majority of LTE network deployments in the EU use the FDD mode of the LTE standard, operating in paired spectrum. Most operators launched first in urban areas, using either the 1800 MHz or 2.6 GHz band, or both as part of a multi-band deployment. Launches of LTE in the 800 MHz band[24] have focused particularly on areas where regulators have mandated certain coverage requirements for winners of spectrum in this band.

In 2010 the EC started a more comprehensive measurement of the status of Information Society development at country level by means of the Digital Agenda Scoreboard (DAS). The DAS includes more than 100 indicators, divided into thematic groups, which illustrate some key dimensions of the European information society (Telecom sector, Broadband, Mobile, Internet usage, Internet services, eGovernment, eCommerce, eBusiness, ICT Skills, Research and Development)[25].

More recently, the EU Commission also introduced as a measurement tool the Digital Economy and Society Index (DESI)[26]. The DESI is a composite index measuring Member States' ICT performance across more than 30 indicators grouped into five categories. The index measures:

— Connectivity: how widespread, fast and affordable broadband is.

— Human capital/digital skills: the level of digital skills of the population and workforce.

— Use of internet: use of online activities from news to banking or shopping.

— Integration of digital technology: how businesses integrate digital technologies, such as e-invoices, cloud services and e-commerce.

— Digital public services: focusing on e-government and e-health.

According to the 2016 DESI, Denmark, The Netherlands, Sweden and Finland are currently the highest performing countries, in Europe and beyond. However, considerable differences still exist across the EU, as shown in the chart below.

According to data published by the Commission in May 2016, in terms of human capital, 45% of people in the EU still do not have any basic digital skills, and 16% of the population has never gone online.

E-Commerce is growing, considering that 53% of the EU population purchases online. However, only 16% of these engage in cross-border purchases. Additionally, European companies that sell online are just 16.7% of total companies in Europe.

TOWARDS A GIGABIT SOCIETY

The European Commission is considering setting new broadband goals for 2025, which would be added to the current Digital Agenda targets[27].

To Cullen's understanding, the ongoing review of the EU regulatory framework for electronic communications could serve as a vehicle to support the broader ambition of a 'Gigabit Society' by 2025, emphasising connectivity. In addition to download speed, this would also address upload speed, high resilience and low latency. Specific goals are to be included in the (non-binding) communication accompanying the review proposal, which is expected in the 4Q 2016.

The Gigabit Society would focus on so-called socio-economic drivers, including key industries, schools, hospitals and universities etc. The connectivity ambition would shape the direction of the framework review and justify key elements, such as spectrum for 5G and regulatory incentives[28] for very high-performance networks. The overarching goal would be ubiquitous connectivity, also along transport routes (connected cars) and providing broadband in rural areas.

IDENTIFYING RELEVANT GAPS IN THE EU LEGAL FRAMEWORK: CURRENT DEBATE

According to the Commission, the current regulatory framework has been broadly successful in creating the conditions for effective competition, but it also notes that the telecom sector is undergoing structural changes, and still suffers from isolated national markets, a lack of regulatory consistency and predictability across the EU, particularly for radio spectrum, with a lack of sufficient investment being felt especially in rural areas.

The Commission plans to review all of the existing legislation and make proposals for change where necessary. Some of the most significant new regulatory challenges are summarised below:

Less regulation in areas with infrastructure competition

According to the Commission, little full "infrastructure competition" has emerged in fixed-line networks, except in very densely populated areas, where cable networks were already present, or where local authorities have been active.

The Commission therefore points out a need for simpler and more proportionate regulation in areas with infrastructure competition (on a national or regional scale). By relaxing the rules, the Commission aims to encourage the deployment of very high capacity networks, while at the same time maintaining effective competition and adequate returns relative to risks.

The Commission also plans to examine the issue of deploying high-speed networks in the most inaccessible areas and to review the Universal Service Directive[29].

Radio spectrum

The Commission notes that a national approach to spectrum management results in widely varying conditions (e.g. different licence duration, coverage requirements). The absence of consistent EU-wide objectives and criteria for spectrum assignment at national level creates barriers to entry, hinders competition and reduces predictability for investors across Europe. Therefore, the Commission concludes that radio spectrum should be managed by Member States under a more harmonised framework.

The European Commission tried to obtain a stronger coordinating role with regard to spectrum authorisations, lamenting a lack of co-ordination among Member States in spectrum assignments and conditions as well as regulatory uncertainty as to the availability of frequencies. However its initial

proposal[30] was not supported by the European Parliament and the Council which finally agreed not to include spectrum in the Regulation for a Telecoms Single Market, adopted in November 2015[31] - as further discussed in Part I, Chapter II.B.

The discussion on the further harmonisation of EU spectrum policy now concentrates on the review of the Radio Spectrum Policy Programme and the review of the electronic communications regulatory framework[32].

Level playing field with OTTs

The Commission acknowledged that telecoms operators compete with services which are increasingly used by end-users as substitutes for traditional electronic communications services (such as voice telephony) but which are not subject to the same regulatory regime.

The review of the telecoms framework will examine means of ensuring a level playing field for all players that provide competing services.

Institutional framework

The Commission also stresses the need to strengthen the institutional framework and to enhance the role of EU bodies in which the regulatory authorities of the Member States are represented, such as BEREC[33] and RSPG[34]. BEREC and the RSPG on their part recognise that effective spectrum management is critical to the Digital Single Market.

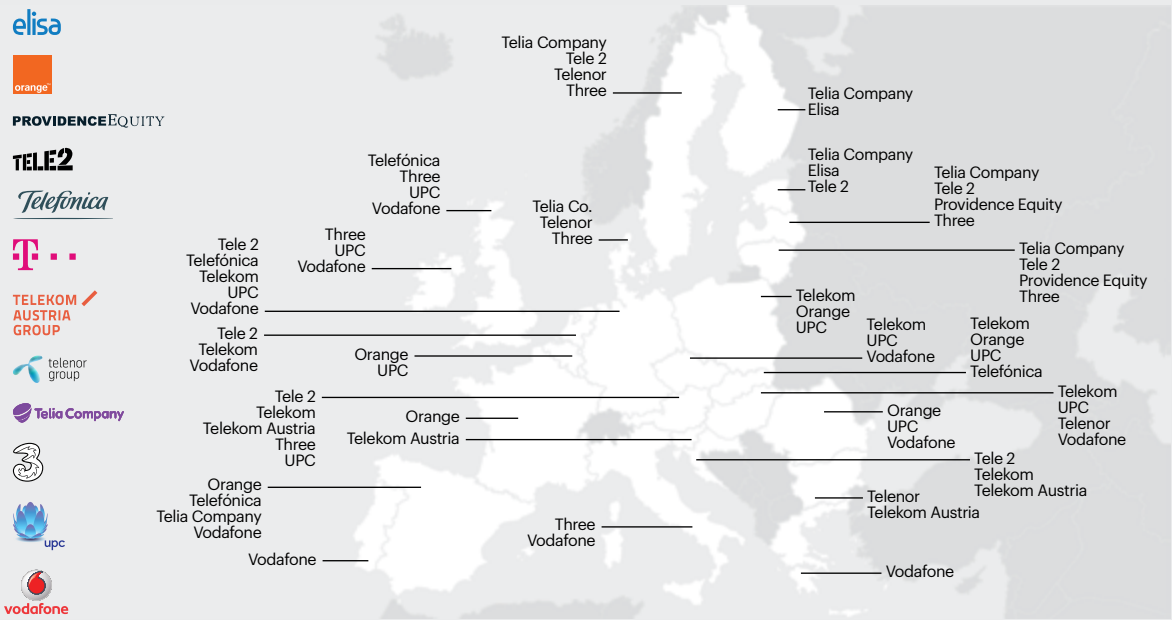
"This co-operation has already brought benefits and it can and should be built upon. BEREC and the RSPG recommend that the Framework Review should seek to enhance such co-operation, such as through the exchange of experiences and the development and dissemination of regulatory best practices as was recently the case with the work on the critical area of spectrum awards", the two bodies recently stated[35].

NATIONAL JURISDICTIONS IN THE GLOBAL INTERNET ENVIRONMENT: INFRASTRUCTURE CHALLENGES

When the European Commission initially proposed a Regulation for a Telecoms Single Market (2013) it pointed out that the existing fragmentation of communications infrastructure into 'national markets' is a barrier to the creation of higher economies of scale, and reduces the growth potential of operators:

> ***"Today, Europe is fragmented into 28 separate national communications markets, each with a limited number of players. As a consequence, while no operator is present in more than half of the Member States, most in far fewer, overall more than 200 operators serve a market of 510 million of customers. EU rules on, for example, authorisations, regulatory conditions, spectrum assignment and consumer protection are implemented in diverging ways.***
>
> ***This patchy scenario raises barriers to entry and increases the costs for operators wanting to provide cross-border services thereby impeding their expansion. This stands in stark contrast with the US or China who have one single market of 330 and 1400 million customers respectively, served by four to five large operators, with one legislation, one licensing system, and one spectrum policy."***[36]

FIGURE 5
Telecommunications groups with presence in multiple EU countries (Cullen International)



The figure below shows the presence of international groups across multiple EU countries. However, no group is present in each of the 28 Member States, and even when a group is present in several countries across the EU, network operation and exploitation are developed within national borders.

UNDERSTANDING INFRASTRUCTURE FRAGMENTATION IN THE EU

Infrastructure fragmentation may be partly explained by the existence of telecommunications infrastructure of former state monopolies. Such infrastructure was built over decades, and, after liberalisation, remained as a 'legacy' of incumbent operators. Incumbents might have changed ownership over time, but a strong national footprint still remains to this day in each of these companies.

Another important element of fragmentation lies in the national assignment of essential resources, such as radio spectrum.

Other obstacles to the creation of a pan-European telecommunications markets must be sought in the different regulatory requirements established by NRAs to address national specificities.

ADDRESSING FRAGMENTATION: TELECOMS SINGLE MARKET (TSM) REGULATION

The Telecoms Single Market Regulation entered into force on 26 November 2015[37].

The Regulation imposes net neutrality rules at EU level from 30 April 2016, and abolishes retail roaming surcharges (subject to the review of the international mobile roaming wholesale market) from 15 June 2017.

The European Commission's initial proposal of 11 September 2013[38] aimed at ensuring a globally competitive European telecoms sector by completing the telecoms single market.

The Commission's plans included several significant changes regarding key policy issues. The European Parliament and the Council have thus been critical about key aspects of the proposal.

All topics except for net neutrality and international roaming (i.e. single EU authorisation, changes to market analysis procedure, EU wholesale broadband products, additional consumer protection measures and BEREC institutional changes), were discarded during the negotiations.

NET NEUTRALITY

Under the EU 2009 regulatory framework for electronic communications, NRAs are allowed to set quality of service parameters on public communications network providers to prevent degradation of service or the slowing down of traffic across networks.

Consumers must be informed —before signing a contract— about the nature of the service to which they subscribe, including traffic management techniques and their impact on service quality, as well as any other limitations.

The TSM Regulation introduces directly binding EU-wide rules on safeguarding open internet access (net neutrality) applying from 30 April 2016. These rules require providers of internet access services to treat all traffic equally, and establish a right of all end-users to access and distribute legal content, applications and services of their choice.

Traffic management

Providers may use reasonable traffic management measures. Such measures are to be based on objective technical requirements, not commercial considerations. Blocking or throttling will be allowed only in a limited number of circumstances listed in the Regulation, for instance to block illegal content, counter a cyber attack or deal with exceptional or temporary traffic congestion.

TABLE 3
Traffic management under the TSM Regulation (Cullen International)

What is allowed?	What is prohibited?
Internet providers may implement reasonable traffic management measures as long as those are: — transparent — non discriminatory — proportionate and — not based on commercial considerations (but on objectively different technical quality of service requirements of specific categories of traffic).	The Regulation prohibits practices such as deep packet inspection. Providers of internet access services must not engage in traffic management going beyond reasonable measures and must not "block, slow down, alter, restrict, interfere with, degrade or discriminate between specific content, applications or services, or specific categories thereof".

Zero rating

Zero rating is a commercial practice used by some providers of internet access, especially mobile operators, not to count the data volume of particular content, applications or services against the user's limited monthly data volume.

The TSM Regulation no longer allows for general bans on zero rating. However, NRAs should assess on a case-by-case basis whether zero rating practices harm end-users by significantly reducing choice.

Recital 7 of the Regulation states that NRAs:

> ***"should be empowered to intervene against agreements or commercial practices which by reason of their scale, lead to situations where end-users' choice is materially reduced in practice. To this end, the assessment of agreements and commercial practices should inter alia take into account the respective positions of the involved providers of internet access services and of content, services and applications."***

This could have consequences in the two Member States that have adopted net neutrality laws which ban zero rating practices outright —the Netherlands and Slovenia. In Norway, zero rating is considered a breach of the guidelines as it would discriminate between different traffic types[39].

Specialised services

Specialised services are "services which are optimised for specific content, applications or services, or a combination thereof, where the optimisation is necessary in order to meet requirements of the content, applications or services for a specific level of quality".

Examples of specialised services are managed IPTV and high-definition video conferencing.

The TSM Regulation avoids explicit references to the term 'specialised services', stating that providers of electronic communications to the public, including providers of internet access services, and providers of content, applications and services "shall be free to offer services other than internet access services".

Under the TSM Regulation, providers may offer or facilitate specialised services, but only if the network capacity is sufficient to provide them in addition to any internet access services provided.

They must not be usable or offered as a replacement for internet access services, and must not have a detrimental effect on the availability or general quality of internet access for end-users.

NRAs will have to closely monitor the market to ensure the continued availability of non-discriminatory internet access at levels of quality that reflect advances in technology. For that purpose, NRAs may impose minimum QoS requirements and other necessary measures[40].

Transparency

The TSM Regulation places additional transparency obligations on providers of internet access services to those already imposed in the 2009 electronic communications regulatory framework. In particular, contracts for internet access services must include some minimum information requirements to end users.

INTERNATIONAL ROAMING

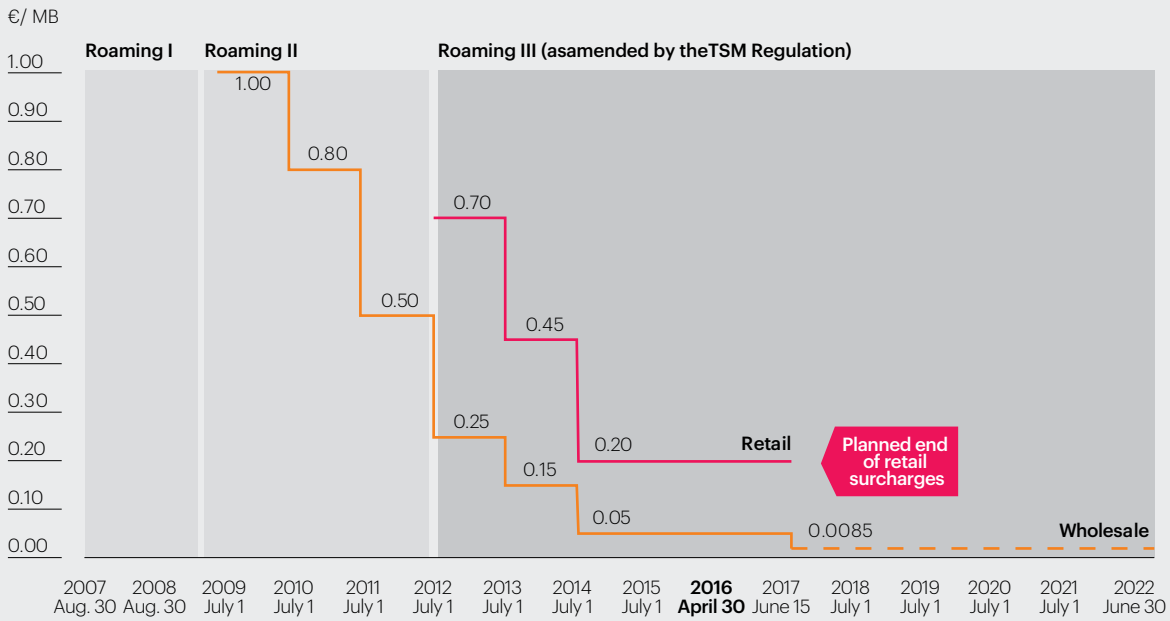
In 2006 the Commission carried out two consultations on a proposed international roaming regulation. It concluded that such a regulation was needed because:

— retail prices for international roaming in Europe remained unjustifiably high and showed no signs of decreasing

— reduction of wholesale prices between operators was not passed on automatically to consumers

— all NRAs found the market for international roaming (M 17/2003, no longer in Commission

FIGURE 6
International roaming maximum charges at EU level (Cullen International)



recommendation on relevant markets) competitive. Therefore, no ex ante regulation had been imposed on wholesale roaming charges. This was due to the market structure that leads to a product market definition covering only national mobile networks

— a single NRA has no powers in relation to both price components of the call: the retail price charged to the end-user in the home country, and the wholesale price charged to the home MNO by the visited MNO in the visited country.

Given the calls from national regulators for action against high end-user prices, there was a risk that divergent national measures could be put in place which would act as a barrier to the single market.

The Commission subsequently acted to cap international roaming surcharges for EU subscribers within the EU by addressing retail and wholesale voice (Roaming I Regulation), retail and wholesale SMS and wholesale data (Roaming II Regulation) and retail data (Roaming III Regulation).

Since then, wholesale and retail international roaming prices have fallen dramatically. Caps for data roaming were introduced in 2009 at the wholesale level, and only in 2012 at the retail level, as is shown in the figure below.

The TSM Regulation goes one step further, abolishing retail international mobile roaming surcharges by 15 June 2017, provided that the Commission has by then fully reviewed the roaming market.

To do so, the Commission had until 15 June 2016 to consult on and produce its review on the wholesale roaming market, including legislative proposals to take effect by the date of abolition in 2017.

If the legislative proposals to resolve any wholesale issues are not applicable by 15 June 2017, the date for the abolition of roaming surcharges will be delayed until the legislation becomes applicable.

In the transitional period leading up to the abolition of roaming surcharges, roaming providers may apply a surcharge in addition to domestic retail price for the provision of regulated retail roaming services, in accordance with caps defined in the Regulation[41].

In the event that a roaming provider was unable to recover its costs from providing regulated retail roaming services, the draft Regulation would allow it to continue applying a surcharge even after the final date for abolition. However, the surcharge could only be to the level required to enable the provider to recover its costs.

The procedure for applying such a surcharge would require the provider to apply for authorisation with a NRA and after potential approval re-apply every 12 months.

According to the regulation, operators may ask roaming customers for 'fair use' of the service to prevent abusive or anomalous usage of regulated retail roaming services by roaming customers, such as permanent roaming.

The Commission is expected to adopt by 31 December 2016 detailed rules on the application of fair use policies and on the methodology for calculating the costs of retail roaming services.

An impact assessment on the EU Roaming regulation was published by the EU Commission in June 2016[42]. The Commission will review the rules every two years from June 2018. The Roaming Regulation mandates NRAs to monitor and supervise compliance with this Regulation, and BEREC to collect data from NRAs on retail and wholesale charges development (notified to the EC twice a year) and to report on the evolution of wholesale prices.

OTHER PROPOSED TSM MEASURES (DROPPED IN THE FINAL REGULATION)

A 'single EU authorisation'

The EU authorisations regime has been considerably simplified since 2002[43]. Operators willing to offer electronic communications services in a given EU country must only notify the start of activities to the NRA authority of the country where they intend to offer services. Nevertheless, the Commission has pointed out that the existing authorisation regime is not sufficiently homogenous across Member States.

When the Commission originally proposed its Telecoms Single Market (TSM) regulation (2013), one of the proposals regarded the creation of a single EU authorisation.

According to that proposal, every European operator would be able to provide electronic communications services in all Member States, based on a single general authorisation and notification in their home Member State. The proposal was discarded during the TSM negotiations. The draft regulation would have fundamentally changed the relationship between NRAs, giving the NRA in the European provider's home Member State a say in several areas that are now the exclusive domain of the local NRAs —a situation that would have led to a complicated division of competences between the 'home' and 'host' NRA.

EC coordination over radio spectrum management

In its first draft of the TSM proposal (2013) the Commission also proposed to create new spectrum coordination responsibility within the Commission itself. In practice, any draft measures by Member States to allow use of spectrum under a general authorisation or to grant individual rights of use would have been subject to prior approval by the Commission.

It also proposed new harmonised procedures for broadband spectrum assignments and use. The Commission wanted NRAs to set timetables

to grant or (re-)assign all spectrum harmonised for use by wireless broadband services through harmonised procedures. The timetables would have applied not only to the assignment of any new bands that may have been harmonised, such as a second digital dividend at 700 MHz, but also to the existing harmonised bands, i.e. the 800, 900 and 1800 MHz, and 2.0, 2.6 and 3.4-3.8 GHz bands.

According to the Commission, setting dates for authorisation procedures well in advance would have created a predictable investment climate and enabled the "synchronised availability" of wireless broadband services within the EU.

This proposal was also dropped from the TSM due to a lack of consensus.

IP INTER-CONNECTION

In the EU, Telecom operators are migrating from circuit switched networks (PSTN) towards Internet Protocol (IP) based packet switched core networks that carry voice, data and video. A converged network for all services reduces the cost of transport and network management.

In the future, all traffic will likely be end-to-end IP. However, during a transitional phase, some services, in particular managed voice services, will continue to use legacy access network equipment, while the core network moves towards IP.

Even in countries where most fixed-line voice customers use voice over broadband (VoB) services managed by their ISPs (i.e. voice traffic is IP native), traditional time division multiplexing (TDM) may still be used for interconnection. This is done by converting IP traffic to/from PSTN by using media gateways.

On the internet, interconnection between ISPs is unregulated and takes the form of IP transit, peering or a combination of these two, in Europe as well as in Latin America.

As summarised in a recent study (H. Galperin, 2016)[44], "Today's Internet architecture is less of a hierarchy than a complex mesh of peering and transit agreements between a more heterogeneous set of network operators (...). Capacity demand is much more geographically distributed across regions, requiring new infrastructure investments outside the traditional Internet's core. (...) The second trend is the rapid growth of traffic volumes...".

The study remarks that the presence of a local IXP is particularly critical for the growth of the Internet ecosystem in emerging countries.

In Europe there is generally no scarcity of Internet exchange points (IXPs).

As of 2014 there were over 50 IXPs operating in Latin America and the Caribbean in 15 different countries. This means that only about a third of the countries in the region (including dependent territories) have an operational IXP.

> ***"The evidence from Latin America suggests that there are several enabling factors for IXPs. First and foremost is a competitive telecommunications market that facilitates entry and promotes competition in domestic transport. Unless transport prices are competitive, local ISPs will have few incentives to invest in infrastructure and exchange traffic at local facilities. In several countries in the region, this basic condition is yet to be met. Second, governments can play a catalysing role by providing political support for the establishment of local traffic exchange facilities".***

Similar conclusions were reached in a recent study (Katz, 2014)[45] which provided eight policy recommendations to promote IXP development in Latin America:

— Ensure the periodic publication of information on the status of IP interconnection, including by use of key performance indicators

— Ensure all countries adopt a standard definition of "internet" —facilitating a more homogenous regulatory treatment across the region

— Regional coordination on indicators, parameters and standards for internet services as well as technical norms on Quality of Service

— Avoid excessive regulation of IP interconnection

— Interconnection should be neutral, non discriminatory and transparent

— Pro-competitive regulation, based on essential facilities and dominance assessments

— Consider interconnection infrastructure within national broadband plans

— IXP as part of (backbone) transmission infrastructure

COORDINATED SPECTRUM POLICIES AND SPECTRUM HARMONISATION AT REGIONAL LEVEL

The EU 2009 regulatory framework for electronic communications includes the definition of an efficient and coordinated spectrum management strategy[46]. Despite the introduced reforms, spectrum policy remains a competence of the Member States.

As for spectrum policies and management, Member States must follow a number of key principles:

Technology and service neutrality

The principles of technology- and service-neutrality allow spectrum users to choose the best technologies and services to apply in the frequency bands which are available for electronic communications services in accordance with the national frequency plans.

The goal is to increase flexibility in spectrum management and access to spectrum.

Allocation of spectrum by the Member States to specific technologies or services should be transparent, proportionate, and non-discriminatory. Member States must regularly review the restrictions to these principles and make public the results of the reviews.

Spectrum hoarding

Competent national authorities may ensure the effective use of spectrum and where spectrum resources are left unused, take action to prevent anti-competitive hoarding. The objective of this provision is to prevent obstacles to new market entry.

Member States may adopt rules to prevent spectrum hoarding, in particular by:

TABLE 4
Technology and service neutrality (Cullen International)

Technology neutrality	Service neutrality
Restrictions to the principle of technology neutrality should be non-discriminatory, appropriate and justified by the need to: — avoid harmful interference (for example by imposing power levels), — protect public health against electromagnetic fields, — ensure technical quality of service, — ensure maximisation of radio frequency sharing, — safeguard efficient use of spectrum or — ensure the fulfilment of a general interest objective.	Measures which require the provision of a specific service in a specific band should be justified to meet clearly defined general interest objectives defined by the Member States in conformity with Community law such as: — the need to promote social, regional and territorial cohesion, — the avoidance of the inefficient use of spectrum, — the promotion of cultural and linguistic diversity and media pluralism, for example by the provision of radio and television broadcasting services. In principle, exceptions should not result in certain services having exclusive use in a given band (as far as possible, other services or technologies should coexist in the same band).

— setting out strict deadlines for the effective exploitation of the rights of use,

— applying penalties, including financial penalties or the withdrawal of the rights of use in the case of non-compliance with the deadlines.

The rules must be proportionate, non-discriminatory and transparent.

Spectrum trading

Member States must ensure that spectrum users can freely transfer or lease their usage rights to third parties in the spectrum bands which the Commission has identified in all Member States (with the exception of frequencies used for broadcasting).

Member States can also decide on spectrum trading in other bands than the ones identified by the Commission.

The following applies:

— Conditions attached to individual rights to use radio frequencies continue to apply after the transfer or lease, unless otherwise specified by the competent national authority.

— Member States may determine that trading does not apply where the individual right to use radio frequencies was initially obtained free of charge (for example, for broadcasting).

— Member States must ensure that the intention to transfer rights as well as the effective transfer is made public. Where spectrum use has been harmonised at EU level, the transfer must comply with such harmonised use.

The Commission, taking utmost account of the opinion of the Radio Spectrum Policy Group (RSPG), may submit legislative proposals to Parliament and the Council for the programmes which will set out the policy orientations and objectives for the strategic planning and harmonisation of the use of spectrum.

The programmes may refer to:

— the availability and efficient use of spectrum, and

— the harmonisation of procedures for the granting of general authorisations or individual rights to use of frequencies.

Parliament and the Council have to adopt the multi-annual spectrum policy programme under the ordinary legislative procedure.

In this framework, the European Commission has been proactively proposing new measures aiming at increasing spectrum policies harmonisation among Member States.

> ***"As regards wireless connectivity, Europe has witnessed significant time lags and differences between Member States in the roll-out of the latest 4G technology, due in part at least to the non-availability of suitable spectrum such as the 800 MHz band. This is accompanied by often wide variations in national spectrum assignment conditions regarding factors of relevance to investment returns and decision-making, such as pricing, licence durations, territorial coverage, spectrum tradability, spectrum caps and reservations and regulated wholesale access to mobile networks (...). The follow-up of the implementation of the Radio Spectrum Policy Programme has revealed[47] considerable lack of coherence across Member States with regard to the authorisation/assignment regimes as well as the availability and the opening and use of spectrum bands on a technology-neutral basis for the provision of wireless broadband connectivity"[48].***

Why spectrum harmonisation matters

Spectrum harmonisation, the uniform allocation of radio frequency bands across countries and regions, and coordinated spectrum policies are key to:

TABLE 5
Spectrum harmonisation bodies and responsibilities (Cullen International)

Organisation	Body	Region		Outcome
		Americas	Europe	
ITU-R	Radio Assembly	Yes	Yes	Inputs for WRC, recommendations
ITU-R	Departments	Yes	Yes	Recommendations, reports
ITU-R	World Radio Conference (WRC)	Yes	Yes	Radio regulations (technical)
EU	RSC	No	Yes	Technical recommendations
EU	RSPG	No	Yes	RSPP, general long term policy
CEPT	ECC and COM-ITU	No	Yes	Technical recommendations, regional inputs for WRC
CITEL	PCC-II: Radio communications	Yes	No	Technical recommendations, regional inputs for WRC
Regulatel	Working group on spectrum management and monitoring	Yes	Yes (Spain, Italy and Portugal)	Information and benchmark on best practices related to spectrum management and monitoring, including the use of new spectrum frequencies.

— avoid interference between services in border areas;

— allow services portability of services using spectrum, i.e. international roaming for mobile services; and

— develop integrated markets for equipment and services, that cut costs for consumers and boost business competitiveness.

Spectrum harmonisation works at different levels: worldwide through the International Telecommunication Union (ITU), and at regional level through different bodies, depending on the region.

Spectrum harmonisation for new services

The last radio conference was held in 2015 (WRC-15) and allocated additional spectrum bands for international mobile telecommunications (IMT) at global and regional level. However, the total identified IMT spectrum in the Radio Regulations, in the three ITU regions, is still below the ITU estimates for the IMT spectrum required by the year 2020[49].

WRC-15 has also decided on the agenda for the next WRC in 2019 which will consider some key steps to boost digital economy development, including by additional IMT spectrum for 5G and beyond; additional RLAN spectrum in the 5 GHz band; and the possible identification of regional/global spectrum bands for railway radio communication systems and Intelligent Transport Systems (ITS).

SPECTRUM HARMONISATION AT EU LEVEL

In Europe harmonisation and spectrum policy decisions result from the interaction of different committees, organisations and European institutions.

The **European Commission** can adopt harmonisation measures on the usage conditions of specific

spectrum bands which apply to all Member States. Furthermore, article 8a.3 of the amended Framework Directive gives the EC the possibility to propose multiannual radio spectrum policy programmes.

The preparation of such measures involves several bodies:

— European Conference of Postal and Telecommunications Administrations (CEPT), providing technical expertise before the decision adoption;

— Radio Spectrum Committee (RSC), providing technical expertise before the decision adoption; and

— Radio Spectrum Policy Group (RSPG), providing an opinion that has to be taken into 'utmost account', but is not binding.

CEPT is an organisation gathering policymakers and regulators from 48 countries across Europe and the former Soviet Union. They collaborate to harmonise telecommunication and radio spectrum among themselves. The CEPT conducts its work through three autonomous committees, two of them related to spectrum issues:

— the Electronic Communications Committee (ECC), developing common policies and regulations in electronic communications and providing information on spectrum use; and

— the ITU working group (Com-ITU), responsible for organising the co-ordination of CEPT actions for the International Telecommunication Union meetings.

The RSC assists the Commission in the development of technical implementing decisions to ensure harmonised conditions across Europe for the availability and efficient use of radio spectrum. The Commission and the Member States collaborate in the RSC through the comitology procedure[50] and regulatory measures are adopted only when a majority of Member States vote in favour.

The Radio Spectrum Policy Group **(RSPG**), established under Commission Decision 2002/622/EC, is a high-level advisory group that assists EU institutions in the development of broader radio spectrum policy issues (rather than the technical measures addressed by the RSC). The group, consisting of national spectrum experts, may also be requested by the Council and Parliament to provide advice on spectrum issues affecting the electronic communications market.

The current Radio Spectrum Policy Programme (**RSPP**) emerged as a compromise between the European Parliament, Commission and Council during the negotiations on the review of the EU 2003 regulatory framework for electronic communications in 2007–2009. It enables Parliament to be involved in the development of general radio spectrum policy, as this used to be a matter between the Commission and Member States.

The RSPP sets out the 'strategic planning and harmonisation of the use of spectrum to ensure the functioning of the internal market' until 2015. The RSPP deals with the long-term strategic, rather than technical, aspects of radio spectrum management for the period 2011-2015. The RSPP is binding on the Member States and they have to report to the European Commission about the measures they take to implement the Programme.

The RSPP main policy goals include:

— making spectrum available for wireless broadband services;

— making an efficient and flexible use of spectrum;

— service and technology neutrality; and

— promoting the least burdensome authorisation regimes.

The Commission was supposed to conduct a review of the programme by 31 December 2015. However, a new RSPP will only be put in place after the review of the EU regulatory framework for electronic communications, for which the Commission is expected to make a proposal by October 2016.

In Europe great effort is being made to achieve spectrum harmonisation, both at high level or broad policies (European Commission and Parliament through RSPG and RSPP) and also in technical decisions and guidelines (EC regulatory procedure with the RSC and CEPT). Member States can participate and vote for or against a given policy or regulation for the duration of the regulatory process, and decisions are taken by majority.

RECENT EC SPECTRUM HARMONISATION MEASURES

As part of its strategy to create a Digital Single Market, in February 2016 the Commission issued a draft decision aiming to coordinate the assignment of the 700 MHz band (694–790 MHz) for wireless broadband services[51]. In order to provide at the same time certainty to providers of audiovisual media services, the Commission proposes to keep frequencies in the sub-700 MHz area (470-694 MHz), as a priority, for digital terrestrial television (DTT) and PMSE equipment, such as wireless microphones used to support the broadcasting of special events.

The Commission's draft decision says that Member States should assign the 700 MHz band to wireless broadband services by 30 June 2020, under harmonised technical conditions set by a (pending) Commission implementing Decision.

The lower part of the UHF band would remain available for DTT and PMSE equipment but Member States would be free to allow the use of the downlink only (i.e. transmission from the network infrastructure to receiving devices) to electronic communication services, to take into account the different relevance of DTT in each country. A review of the use of the sub-700 MHz band would take place by 1 January 2025.

Once approved, the decision will be directly binding on Member States following its adoption by the European Parliament and the Council.

Over the years, the European Commission has taken several harmonisation decisions, including, among others:

— **800 MHz band** (first 'digital dividend'). In May 2010 the Commission adopted a (binding) decision on the harmonised use of the 800 MHz band. It does not require Member States to open the band for telecommunications services nor set a deadline for doing so. But if/ when a Member State does decide to open up the 800 MHz band, it must follow the technical conditions set by the decision[52].

— **900 and 1800 MHz bands:** Decision on UMTS of October 2009. The decision defines harmonised technical measures to enable the use of the 900 and 1800 MHz bands previously designated to GSM services ('the GSM bands') for UMTS and other more advanced technologies that can coexist with GSM[53].

— **Decision on WiMAX and LTE in the 900 and 1800 MHz bands** of April 2011. The Commission adopted its decision obliging Member States to allow the use of LTE and WiMAX, both 4G mobile technologies, in the 900 and 1800 MHz bands[54].

— **1.5 GHz (L band)**. Commission decision of 8 May 2015 on the harmonised designation of the 1.5 GHz (1452-1492 MHz) for wireless broadband in downlink-only mode. Member States must designate and make available, on a non-exclusive basis, the 1452-1492 MHz for terrestrial systems capable of providing electronic communications services within six months of the decision[55].

— **Radio spectrum for short-range devices**. Commission decision of December 2013[56] that harmonises 81 frequency bands covering 15 categories of devices that can play a role in the IoT and is expected to be modified by mid-2016.

— **Radio frequency identification (RFID).** Even when several frequency bands are available for RFID systems on an unlicensed basis; the Commission has adopted a decision on

harmonisation of the radio spectrum for RFID devices operating in the ultra high frequency (UHF) band[57] that imposes an obligation on Member States to designate and make available specified frequency bands for RFID by June 2007. However, as the use of RFID increases, long-term requirements for additional spectrum may arise. The Commission states that it may use its powers under the radio spectrum decision to identify additional harmonised spectrum.

STANDARDS AND INTEROPERABILITY AT REGIONAL LEVEL

As new digital services develop worldwide, common standards and interoperability between service providers and locations are perceived as key.

Service interoperability, interconnection, and the use of open standards have several benefits, such as:

— encouraging innovation and the development of new business models;

— building network benefits;

— reducing development and research cost;

— allowing greater economies of scale generating efficiencies for device providers;

— lowering barriers of entry to the market;

— fostering innovation;

— providing mobility and service portability between countries;

— increasing consumer choice by allowing integration flexibility;

— and decreasing consumers' fear of obsolescence.

Interoperability is also important for new service developments in the digital economy including Internet of Things (IoT) services.

Global standardisation bodies include the ITU-T, the 3GPP, GSMA, the Internet Engineering Task Force (IETF) and IEEE. In the framework of IoT development many other industry coalitions have emerged, including the Industrial Internet Consortium, Open Interconnection Consortium, ZigBee Alliance, and AllSeen Alliance, among many others.

The variety of organisations and bodies involved turns standardisation into a costly and complex process. In the following years we are likely to observe a mismatching path towards standardisation with overlapping initiatives, conflicting protocols and a possible fragmentation of IoT services.

WHAT IS THE EU'S ROLE IN NEW SERVICES' STANDARDISATION?

The EU supports an effective and coherent standardisation framework —the EU regulation on European standardisation[58] sets the legal framework of the standardisation system. In addition, the Commission financially supports the work of the three European standardisation organisations:

— ETSI – the European Telecommunications Standards Institute

— CEN – the European Committee for Standardization

— CENELEC – the European Committee for Electrotechnical Standardization.

INTEROPERABILITY AND STANDARDISATION IN THE DSM STRATEGY

The Digital Single Market strategy includes interoperability and standardisation in the pillar on 'maximising the growth potential of the European Digital Economy'.

The European Multi Stakeholder Platform on ICT Standardisation[59] advises the Commission on matters relating to the implementation of ICT standardisation policy in different fields.

The 2016 rolling plan for ICT standardisation goes through:

— **Societal Challenges:** eHealth, accessibility of ICT products and services, web accessibility, e-Skills and e-Learning, emergency communications and eCall.

— **Innovation for the Digital Single Market:** e-Procurement, e-Invoicing, card/internet and mobile payments, eXtensible Business Reporting Language (XBRL) and Online Dispute Resolution (ODR).

— **Sustainable growth:** Smart grids and smart metering, smart cities, ICT environmental impact, European Electronic Toll Service (EETS) and Intelligent Transport System (ITS).

— **Key enablers and security:** Cloud computing, (Open) Data, e-government, electronic identification and trust services including e-Signatures, Radio Frequency Identification (RFID), Internet of Things (IoT), network and information security (cybersecurity) and ePrivacy.

3 —
ACCESS TO ONLINE GOODS AND SERVICES IN THE EU

E-COMMERCE: PROTECTING CONSUMER RIGHTS IN THE DIGITAL WORLD

Although online sales continue increasing, the EU is aware that the achievement of an integrated European e-commerce market is far from being a reality.

Recent statistics show that most European consumers feel confident about purchasing online from a retailer located in their own country, whereas only 36% feel confident about purchasing from another European country[60].

On the businesses' side, in 2014 the international online sales made by EU companies only amounted to 15% of their revenues, of which 10% came from other EU countries[61].

Internet companies and start-ups cannot take full advantage of growth opportunities online, and whereas the US-based online services account for 54% of the online commerce in the region, only 7% of SMEs sell cross-border[62].

ONLINE CONTRACTS: EU STATUS AND CURRENT DEBATE

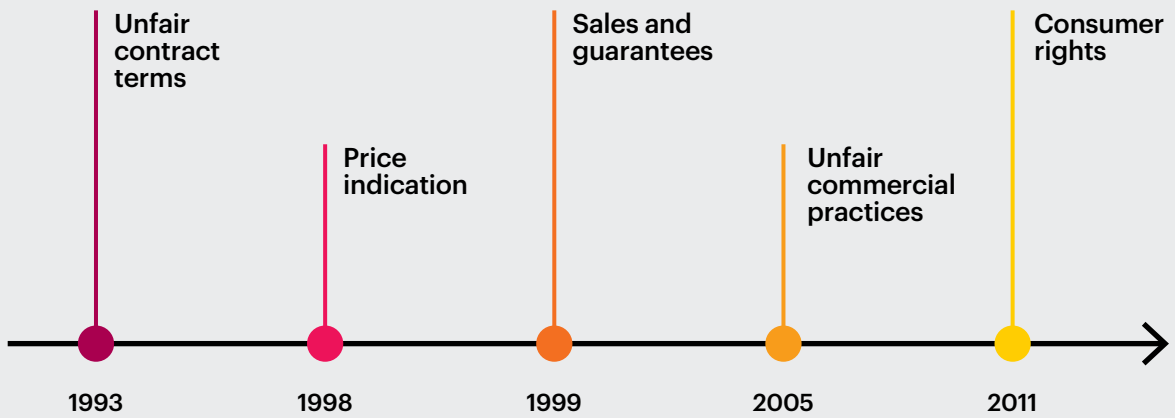
Online retailers with an establishment in the EU benefit from the freedom to provide services throughout the EU[63]. This implies that they can provide their services freely throughout the entire EU territory.

According to the e-Commerce Directive[64], Member States must not restrict this freedom, for instance by making providers subject to a prior authorisation or other equivalent requirements[65]. Thus, online retailers benefit from a country of origin principle.

In contrast, the application of consumer rules is normally based on the country of destination principle. This means that contracts between a consumer and an online retailer are ruled by the law of the country where the consumer resides[66].

For example, when an online retailer established in France targets a Spanish consumer, it is bound by

FIGURE 7
Gradual harmonisation of consumer rules in the EU (Cullen International)



the Spanish legislation on consumer protection. In practice, this implies that online retailers targeting consumers across the entire EU have to comply with 28 different consumer protection frameworks.

The lack of knowledge of the rules that have to be followed in other countries is one of the obstacles preventing companies from increasing their cross-border online sales[67].

The EU has been gradually harmonising different rules on consumer protection, as shown in the graph below.

The Consumer Rights Directive (CRD)[68], which entered into force on 13 June 2014, is currently the main EU instrument on consumer protection, including online. Previous directives on consumer protection allowed Member States to introduce higher standards of protection (minimum harmonisation).

However, the CRD prevents Member States from introducing in their national laws consumer protection standards which are higher than those set forth in the directive (full harmonisation)[69].

The CRD harmonises aspects such as pre-contractual information requirements for distance contracts[70] and the consumer's right of withdrawal[71]. However, aspects such as the language in which contractual information has to be provided to the consumer have not yet been harmonised[72].

Furthermore, the Commission is conducting a fitness check of the entire EU horizontal consumer legislation (including the CRD) in order to determine whether it is still fit for purpose[73].

FIGURE 8
Examples of discriminatory practices a French consumer faces when buying online (Cullen International)

Non-discrimination principle

Traders often put barriers to the free movement of goods and services in the EU for purely commercial reasons, and without objective justifications.

This happens when traders operating in an EU country block or limit the access to their online interfaces (e.g. webs, apps) of customers from other Member States. This practice is known as geo-blocking.

Additionally, traders often apply other discriminatory practices similar to geo-blocking that artificially segment the EU internal market.

The Services Directive prohibits online service providers from applying discriminatory provisions to consumers based on their nationality or place of residence[74]. This directive intends to allow, for example, a French consumer to buy from a website in Belgium under the same conditions as a Belgian consumer.

Differences in treatment can be justified if they are based on objective business considerations (e.g. market conditions such as higher or lower demand influenced by seasonality, delivery costs)[75].

According to the Commission, this non-discrimination principle has proven difficult to enforce in an effective manner[76].

Thus, the European Commission presented on 25 May 2015 a legislative proposal to prohibit traders from discriminating against customers (both

TABLE 6
Prohibited discriminatory practices in online trade (Cullen International)

Issue	Prohibited discriminatory practice
Access to online interfaces (e.g. websites, apps)	— Blocking or limiting customers' access to the trader's online interface. — Redirecting customers to a version of the trader's online interface which is different from the online interface the customer originally tried to access, unless they give their consent prior to the redirection.
General conditions of access (e.g. prices, terms and conditions) to goods and services	Applying different general conditions of access when the trader: — sells goods which are not delivered by him to the Member State of the customer (thus when a Spanish customer wanting to buy a car finds the best deal on a German website, she should be able to order it and collect it at the trader's premises or organise delivery herself to her home); — provides electronically supplied services, excluding those providing access to copyright protected works and also those provided by small enterprises (thus an Italian customer wanting to buy hosting services for his website from a French company should be able to buy the service without paying additional fees compared to a French customer); — provides other services which are supplied where it operates, in a Member State other than that of the customer (thus a Finnish family visiting an amusement park in the Netherlands should be able enjoy the same price as a Dutch family).

consumers and traders) buying online and offline for reasons related to their nationality, residence or establishment[77]. In essence, the proposed regulation defines the situations where traders would be prevented from discriminating between customers (consumers and traders alike) for reasons related to their nationality, place of residence or place of establishment. Some of the prohibited discriminatory practices are summarised below.

It is worth noting that the proposed regulation would not apply to audiovisual and electronic communication services and would also partially exclude copyright related services, as seen in relation to the different conditions of access.

Other recent EU initiatives

The European Commission believes that new rules for online cross-border purchases would encourage businesses to sell online across borders, and would increase consumer confidence in cross-border e-commerce[78].

As part of the DSM strategy, in December 2015 the Commission gave a new push to the process of harmonisation of rules on contracts and consumer protection.

In particular, the Commission proposed two directives that, if adopted, would fully harmonise certain aspects of business-to-consumer (B2C) online contracts for:

— the supply of digital content[79]; and

— the online and other distance sales of goods[80].

The aspects of contracts that would be harmonised cover:

— conformity of the digital content/good with the contract;

— remedies available in the case of lack of conformity; and

— modification or termination of the contract.

In parallel to these legislative proposals, at the level of enforcement, the Commission has proposed to review the functioning of the network of national authorities responsible for enforcing EU consumer protection laws[81].

The purpose of this network is that national authorities cooperate and coordinate their approach on the the application of consumer protection law.

In a new legislative proposal presented in May 2016[82], the Commission is proposing that national authorities have a further number of minimum powers to tackle intra EU cross-border infringements of consumer rights (i.e. which harm or potentially harm the collective interest of consumers residing in an EU country other than the country where the infringement took place), and in particular to:

— make test purchases and carry out mystery shopping;

— require the supply by any person or company (i.e. banks, internet service providers, domain name registries, registrars, hosting service providers) of any information to identify persons involved in financial and data flows, ownership of websites, etc.;

— adopt interim measures;

— block websites;

— impose penalties.

Also, the legislative proposal would put in place a stronger coordination mechanism to tackle practices which harm a large majority of EU consumers (in 75% of Member States or more that amount to 75% of the EU population or more). The Commission would be given a role to coordinate common actions by national authorities to stop such practices.

Furthermore, on February 15, 2016 the Commission launched the Online Dispute Resolution platform[83] to help EU consumers and traders solve disputes over (domestic and cross-border) purchases made online without going to court.

DIGITAL SIGNATURE

Since 1997, the Commission has identified electronic signatures as an essential tool for providing the necessary security and trust for the conduct of electronic transactions on the Internet.

The Commission proposed a directive on electronic signatures in 1998, adopted a year later, to avoid a fragmentation of the internal market that could have resulted from the adoption of divergent national regulations[84].

The Commission has however recognised that the use of electronic signatures has been much less prevalent than expected and the market is not well developed.

In its DSM strategy[85] of May 2015, the Commission highlighted the importance of trust and security as critical factors for people, businesses and governments to go digital. According to the Commission, electronic identification (eIDAS) is key to boosting trust and convenience in secure and seamless cross-border electronic transactions in very different sectors like banking, healthcare, the sharing economy, transport and public administration.

The eIDAS Regulation[86] on electronic identification and trust services adopted in July 2014 aims at allowing individuals and businesses to use their own electronic identification schemes (eIDAS) to interact with public administrations. The objective is also to modernise the rules on electronic signatures and to ensure that related online services (so-called "trust services"), such as time stamping, electronic delivery, electronic seals and website authentication work across borders, have the same legal status as traditional paper-based processes.

By 1 July 2016, the rules on trust services will take effect and repeal the existing Electronic Signature Directive of 1999[87]. In addition, an EU trustmark for qualified trust services will tell internet users whether they can trust a service online.

The rules governing the recognition of eID between Member States have already been applicable since

September 2015, and will become mandatory from September 2018 onwards.

E-PAYMENTS

Electronic payments and electronic money are alternate payment methods designed to increase the coverage of banking transactions and services.

Electronic payments (e-Payments) refers to means of payment through electronic platforms or devices. They encompass transactions generated on web pages and apps; on desktops, tablets or mobile phones.

As part of a broader e-Payment definition, mobile payments (m-Payments) refers to e-Payments performed through mobile devices, mainly smartphones.

The Payment Services Directive[88] (PSD2) adopted in November 2015 aims at pushing forward EU online and mobile payments that are suffering from an important unrealised potential compared to other parts of the world although they are considered as key drivers of e-commerce in Europe. According to the Commission, the European electronic and mobile payment market is fragmented, lacks transparency, competition and interoperability.

As from November 2017, PSD2 will replace the current Payment Services Directive (PSD). The new directive will regulate at EU level for the first time internet-based "payment initiation services" (PIS). PISs allow consumers to buy online without the need for a credit card by providing a software bridge between the bank account of the user and the merchant.

PISs are already offered in a number of Member States (e.g. Sofort in Germany, IDeal in the Netherlands, Trustly in Sweden).

Some types of mobile wallet apps, including ones combined with Near Field Communications (NFC), would also fall under the definition of PIS when the transactions are charged directly to the user's bank account.

PIS providers will have to follow the same rules as traditional payment service providers: registration or licensing (depending on the amount of transactions handled) and supervision by the competent authorities.

In addition, new security requirements in PSD2 will oblige all payment service providers to step up the security around online payments. In particular, PSD2 requires payment service providers to apply strong authentication measures (combining at least two user identification mechanisms) in order to increase security and trust in electronic payments. The European Banking Authority (EBA) has been mandated by the European Commission to develop 'open technical standards' aimed at ensuring strong authentication for electronic payments. Once adopted by the Commission, these new security standards would have to apply as from September 2018.

Finally, PSD2 also updates the exclusion for payments through telecoms operators that are charged to the user's telephone bill. The exclusion now covers payments made through telecom operators for the purchase of digital services such as music and digital newspapers that are downloaded on a digital device or of electronic tickets or donations to charities. Only payments under a certain threshold are excluded (€50 per transaction; €300 per billing month).

TAXATION OF DIGITAL GOODS AND SERVICES

Direct taxation of companies and individuals is still within the competence of the Member States and thus is not governed by EU rules. One of the main outcomes, which regards all sectors of the economy, is that businesses may seek to practice tax optimisation techniques.

However, the EU Treaties authorise the EU to approximate national regulations on direct taxation as they directly affect the functioning of the Internal Market.

Several EU countries have complained about the way certain corporations, especially in the digital economy sectors, generate huge profits in their countries but have their tax base in other EU countries where corporate tax rates are lower.

Value added tax

The EU has a system of value added tax (VAT) that applies to (more or less) all goods and services that are sold for use or consumption in the EU.

Goods and services which are sold for use or consumption outside of the EU are normally not subject to VAT. Conversely, imports are taxed to keep the system fair for EU producers so that they can compete on equal terms in the EU market with suppliers situated outside the EU.

The EU institutions do not collect the tax, but rather each EU Member State is required to adopt a VAT that complies with the EU VAT Directive[89]. The standard VAT rate must be at least 15% and the reduced rate at least 5% (only for supplies of goods and services referred to in an exhaustive list).

Currently, the standard VAT rates applied by Member States range from 17 to 27%[90].

Cross-border sales

Importantly for cross-border sales, including e-commerce, VAT is charged at the rate applicable in the EU country where the customer is located (rather than the country where the supplier is established).

The European Commission announced, as part of its Digital Single Market strategy[91], plans to present by the end of 2016 legislative proposals to modernise and simplify VAT for cross-border e-commerce.

One of the main elements of these proposals will be to extend the so-called mini one-stop shop (MOSS)[92]. The MOSS, which was established in 2015, allows businesses that sell digital services to customers in more than one EU country to declare and pay all the VAT due via a web portal in their own Member State (instead of registering for VAT in each Member State in which they have customers). The Commission will propose to extend the MOSS to cover tangible goods which are sold online.

Unequal treatment of paper versus e-publications

The European Commission will also propose to amend the VAT Directive so that e-books can benefit from the same reduced VAT rates as printed books.

While the average VAT rate for print books across the EU is 7.6%, the corresponding rate for e-books stands at 19.9%, thus placing them at a disadvantage[93].

The Court of Justice of the EU ruled in March 2015 that France and Luxembourg could not apply a reduced VAT rate on e-books[94]. The court confirmed that an e-book is an *"electronically supplied service"*. These services are excluded from Annex III of the VAT Directive which lists the goods and services which can benefit from a reduced VAT rate.

Following this ruling, a number of Member States and the European Parliament have called on the Commission to address the unequal treatment of paper versus e-publications for VAT purposes.

COPYRIGHT

Copyright is a significant part of intellectual property rights. Since the Berne Convention (1886), countries have expressed a common desire to offer an effective, and as uniform as possible, protection for literary and artistic works. Every production in the literary, scientific and artistic domain, whatever may be the mode or form of its expression, enjoys copyright protection.

Books and other writings, music, films, photographic works, sound records and broadcasts are examples of protected works. Protection is automatically conferred to creative works, independently of prior registration or level of novelty. Whereas some countries may require fixation in a tangible or intangible medium to confer protection to works (and assure protection cannot be conferred merely to ideas), originality is the main requirement for protection in most of the jurisdictions.

Copyright grants creators the exclusive right to reproduce their work in material forms, hard and digital, as well as to publish, perform in public, communicate to the public, translate and adapt works. Authors normally do not have the means to carry out the exploitation of their works by themselves, choosing to licence the exercise of these rights to intermediaries, such as publishers, record companies, film studios, broadcasters and copyright collecting societies.

Incentives for creativity have always been the primary reason for the establishment of copyright systems. Besides that, the right to exclude others from using the work (exclusivity) has paved the way for the recovery of investments made by intermediaries, leading to the creation of copyright industries.

Piracy

The phenomenon of online piracy (e.g. of music, films, e-books) has evolved over the years. The use of and the revenues from the new digital distribution channels of copyrighted material have shown constant growth in recent years. Rights holders see digital piracy as a big threat to the development of the creative industries.

Territoriality

Rights holders enjoy exclusive territorial rights. Ownership of such rights may vary from region to region, as content producers and distributors may wish to enter into a great number of agreements in order to cover a broader geographical area and raise profits by exploiting their copyrighted works worldwide. Some copyright licence agreements already foresee distribution in "the territory of the universe", as a means to assure the granting of such rights.

Based on exclusivity and on the fact that exclusivity is commonly delimited by a geographical area, content owners have found ways to protect their content online with the help of technological measures of protection, one of them commonly known as geo-blocking.

Geo-blocking

Geo-blocking is a practice that restricts access to internet content based on the user's geographical location, normally identified by the user internet protocol (IP). The identification of the localisation of the user is done with the help of geo-location techniques, such as checking the user's IP address against a black or white list, the result of which is then used to determine whether the system will approve or deny access to the content.

Premium content on the internet, such as films and television shows, are the primary target for protection by geo-blocking. The practice is also commonly seen in the games industry.

The European Union is currently dealing with geo-blocking issues under the fields of consumer and electronic services. Audiovisual and other copyright related fields are expressly excluded from the proposed regulation and will be addressed in September 2016. In the audiovisual field, only geo-blocking practices to restrict the consumer's access to subscribed content while traveling to another EU country have been addressed so far.

Legislators worldwide are dealing with geo-blocking discussions by assessing the issues from both sides' perspectives, thus struggling to coordinate reform of consumer and intellectual property laws.[95] The concept of geo-blocking may also vary from jurisdiction to jurisdiction, with some countries considering the automatic rerouting of users to local versions of websites also as a way of blocking access to the URL typed. Further measures such as allowing access, but blocking purchases from specific IP locations are not considered as geo-blocking measures.

AUDIOVISUAL CONTENT: GEO-BLOCKING AND EXCLUSIVITY RIGHTS

One of the objectives of the European Commission Digital Single Market strategy is to allow *"wider online access to (copyright-protected) works by users across Europe"*.

Although rights of authors and other rightsholders have been largely harmonised at the EU level (in particular by the 2001 EU Copyright Directive)[96], the territoriality of copyright is still at the core of the EU copyright framework.

Each Member State grants copyright protection in its own territory according to national legislation and, as a result, providers of online content services must buy the rights in each EU Member State where they want to make content available.

As explained in the European Commission Copyright Action Plan of 9 December 2015[97], the creation of a unitary European Copyright Code, which would totally harmonise the area of copyright law in the EU and replace national laws, remains for the time being a "long-term vision".

The territoriality of copyright and the related difficulties for content service providers to clear rights in multiple territories are identified by the European Commission as part of the obstacles to a wider cross-border circulation of audiovisual works in the EU.

Additional barriers would result from copyright licensing practices (so-called territorial exclusivity) which are usually privileged by audiovisual producers when selling rights to premium content. The same licensing practices are commonly applied by football leagues to sell premium sport rights.

To recoup high upfront (i.e. pre-production) investments, audiovisual producers grant (more profitable) exclusive licences to single distributors or service providers (usually for a specific release window, e.g. video on demand or pay TV) in each Member State in exchange for pre-financing.

According to the European Commission, copyright territoriality, combined with territorial and exclusive licensing, prevents service providers from acquiring a licence covering additional territories to the one they primarily focus on. To comply with contractual clauses in content licensing agreements they therefore need to block online access by users in other countries, including their own subscribers when temporarily abroad (so-called 'geo-blocking').

It is worth noting that the proposed Geo-blocking Regulation excludes audiovisual services from its scope of application.

Audiovisual producers, distributors and commercial broadcasters deny the assumption according to which a revision of the EU copyright framework would pave the way for multi-territorial distribution. They argue that EU language and cultural diversity requires focus primarily on national audiences (or

at best on common language groups) and cross-border demand is often too low to offset the high costs of cross-border distribution (e.g. targeted marketing activities). In addition, any legislative initiative mandating licensing structures or limiting contractual freedom would have a negative impact on the producers' ability to finance content.

EU Commission addresses content services portability as a first step

In view of the highly polarised debate around copyright territoriality and exclusive licensing practices, the Commission has proposed in its Copyright Action Plan a gradual approach, which balances the objective of removing obstacles to cross-border access with the need *"to ensure viable financing models for those who are primarily responsible for content creation"*.

Along the same lines, the European Parliament (own-initiative) resolution of 9 July 2015 on the implementation of the EU Copyright Directive had mentioned the need to end unjustified geo-blocking and foster cross-border online services while at the same time protecting the financing of audiovisual and film productions, which are still based on the territoriality of rights.

In its Copyright Action Plan, as a first step, the Commission proposes that a new right should be given to consumers to access online (audiovisual and other) content services they have purchased or subscribed to at home while they are temporarily present in another EU country.

According to the Commission, this proposal does not challenge the territoriality of copyright, as it introduces a legal fiction according to which the relevant copyright acts would be deemed to occur only in the user's country of residence.

Service providers would be obliged to offer to their subscribers (when temporarily abroad) cross-border portability and any clause in contracts with rightsholders limiting or prohibiting portability would be considered void. To avoid disproportionate burdens, the portability obligation would apply only to providers that already verify the user's country of residence (i.e. all paid-for services and only certain free services).

This proposal is currently being debated in the European Parliament and Council, which are expected to reach an agreement by the end of 2016. Both institutions seem to broadly agree on the aim of the Commission proposal and discussions are mostly focusing on how to avoid abuses by users. Following adoption by Parliament and Council (by co-decision procedure), obligations will be directly applicable in all Member States after a transition period.

Expected next steps to allow wider online cross-border access

The next step of the European Commission's plan to enhance cross-border access to audiovisual content across the EU is expected to be included in a second copyright package to be proposed in September 2016[98].

One option under review is the extension to the online distribution of TV programmes of the simplified rights clearance mechanisms that were set out in 1993 to boost cross-border satellite broadcasting and cable retransmission (Satellite and Cable Directive)[99]. In particular:

— the so-called 'country of origin principle' would be applied to the licensing of rights for online distribution of TV programmes. This principle allows broadcasters to acquire licences for cross-border satellite broadcasting only in the country where the TV signal is introduced;

— the so-called 'cable retransmission clearance system' would be applied to other online retransmissions. This system requires all rightholders (with the exception of broadcasters) to exercise their cable retransmission rights through collecting societies, including rightholders that have not transferred their rights to a collecting society.

To Cullen International's understanding the scope of such an initiative would be limited to facilitate the cross-border availability of online services including TV programmes (e.g. catch-up TV services, rather than film video-on-demand services)[100].

The results of the ongoing Commission antitrust proceedings, which were opened in July 2015 against six major film studios and a pay TV operator, are also expected to have a significant impact on EU cross-border availability of audio-visual content.

The case concerns content licensing agreements (which typically cover only one EU Member State or common language area) that would prevent a pay TV operator from responding to unsolicited requests (passive sales) for its pay TV services (including online) from consumers located outside of the country it targets.

FIGHTING ONLINE PIRACY

There are different forms of copyright infringement observed in the online digital ecosystems. Among the most relevant ones, we observe:

— File sharing by means of cyberlockers (cloud storage space with possibility of cash payments to incentivise the illegal upload of popular content), peer-to-peer (P2P) networks.

— File sharing and streaming by means of user-created websites.

— 'Leech sites', which use a mask to access content available at a UGC (user-generated content) site.

— Deep linking or hyperlinking.

— More conventional means such as FTP (file transfer protocol), webserver, IRC (internet reality chat) or Usenet.

— Use of Virtual Private Networks (VPNs) and other means of unblocking access to geo-blocked content.

— OTT piracy by password sharing among users.

There are several possible regulatory approaches in tackling online piracy. For some of these measures, regulatory authorities may have a role to play.

— Blocking of websites by mere conduit (internet access) providers (this refers to a general obligation imposed by law and not by court injunctions imposing blocking in specific cases).

— Measures against downloaders, typically, involving some sort of graduated response mechanisms.

— Taking-down of unauthorised copyright content by hosting providers.

— Developing legal offers: attractive online and legal cultural services for users which at the same time are a sustainable business model for rightsholders

— Other measures: such as injunctions adopted by courts, awareness raising and other measures.

FIGHTING ONLINE PIRACY IN THE EU

The current Intellectual Property Rights Enforcement Directive (IPRED)[101] and the Copyright Directive[102] require EU countries to apply remedies and penalties against those engaged in piracy and to the benefit of those holders of intellectual property rights willing to protect their rights.

Additionally, the e-Commerce Directive harmonises the conditions under which information society service providers can be held liable for third party illegal content when they act as 'online intermediaries'[103].

The directive states, as a general principle, that Member States may not impose on intermediaries a general obligation to monitor third party information they transmit or store. At the same time, when illegal content is identified, intermediaries should take effective action to remove it.

The magnitude of online piracy is still a big concern for both the EU and its Member States. Estimated value losses due to piracy in the creative and cultural industries are as follows:

— cumulative value loss in the range of about €35bn to almost €50bn; and

— cumulative job loss between 0.2m and 1m jobs over the 2008-2011 period[104].

RECENT AND UPCOMING INITIATIVES

In December 2015, the Commission adopted an action plan[105] to modernise the EU copyright rules, which further clarified expected upcoming initiatives on IPR enforcement:

'Follow-the-money' approach

The Commission has engaged all concerned parties in setting up and applying self-regulatory 'follow-the-money' mechanisms. The aim is to disrupt the money trail for commercial-scale intellectual property infringing activities and to make them economically unviable.

On 14 March 2016 the Commission held a Stakeholders' meeting on online advertising and IPR. Stakeholders (such as representatives of the advertising industry, intermediaries, and rightsholders) discussed the possibility of establishing a voluntary agreement at the EU level to avoid the placement of advertising on websites infringing copyright.

Review of IPRED

The European Commission is considering a review of IPRED focusing on commercial-scale infringements and clarifying the rules for identifying copyright infringers, the application of provisional and precautionary measures and injunctions and their cross-border effect, the calculation and allocation of damages and legal costs.

Liability of platforms

The European Commission published on 25 May 2016 a communication[106] setting out its position on how online platforms should be regulated.

Online platforms cover a wide range of activities including online marketplaces, search engines, social media, and video and content-sharing sites. These platforms operate in multi-sided markets and facilitate interactions (including commercial transactions) between different groups of users.

The communication does not propose a new general law on online platforms, nor does it suggest changing the liability regime set out by the e-Commerce Directive. However, the Commission presented a number of targeted measures.

In particular, the communication says the Commission will assess the need for:

— guidance on whether online platforms would still benefit from the exemption from intermediary liability in the e-Commerce Directive when they put in place voluntary measures to fight illegal content online; and

— notice-and-action procedures to take down illegal content (after taking due account of the updated audiovisual media and copyright frameworks)

Currently, procedures for removal of copyright infringing content online vary from one EU country to another.

PRIVACY AND DATA PROTECTION

EW EU DATA PROTECTION RULES

Recent statistics in Europe show that the vast majority of EU citizens have concerns over the way their personal data is processed[107]. For instance:

— The majority of people are uncomfortable about internet companies using information about their online activity for the purposes of targeted advertising.

— 69% of EU citizens consider that their explicit approval should be required in all cases before their data is collected and processed.

— Only 22% of Europeans have full trust in companies such as search engines, social networking sites and e-mail services[108].

With the purpose of increasing trust in digital services by better protecting the personal data of European citizens[109], the EU adopted on 14 April 2016 new EU-wide data protection rules[110].

The General Data Protection Regulation (GDPR), which will apply from 25 May 2018, will replace the current Data Protection Directive[111].

The Data Protection Directive, which dates back to 1995, recognises the free movement of personal data in the EU and, at the same time, establishes a high level of protection for the privacy of individuals.

The Data Protection Directive is complemented by the e-Privacy Directive[112], which contains specific rules on the processing of personal data and the protection of privacy in the electronic communications sector. Most of its provisions only apply to providers of public electronic communications services.

The European Commission, which is currently reviewing this directive, is considering extending its scope to OTT services that provide services competing with those of telecoms operators (e.g. WhatsApp)[113].

The provisions in the Data Protection Directive had to be transposed into national laws and Member States were allowed to set higher data protection standards in their national legislation.

As a result of this, currently 28 inconsistent national data protection laws coexist in the EU. Thus, companies have to comply with different data protection laws in the Member States where they provide their services.

The GDPR is going to put an end to this legal fragmentation as its provisions, which will not require national implementing laws, will be directly applicable throughout the EU.

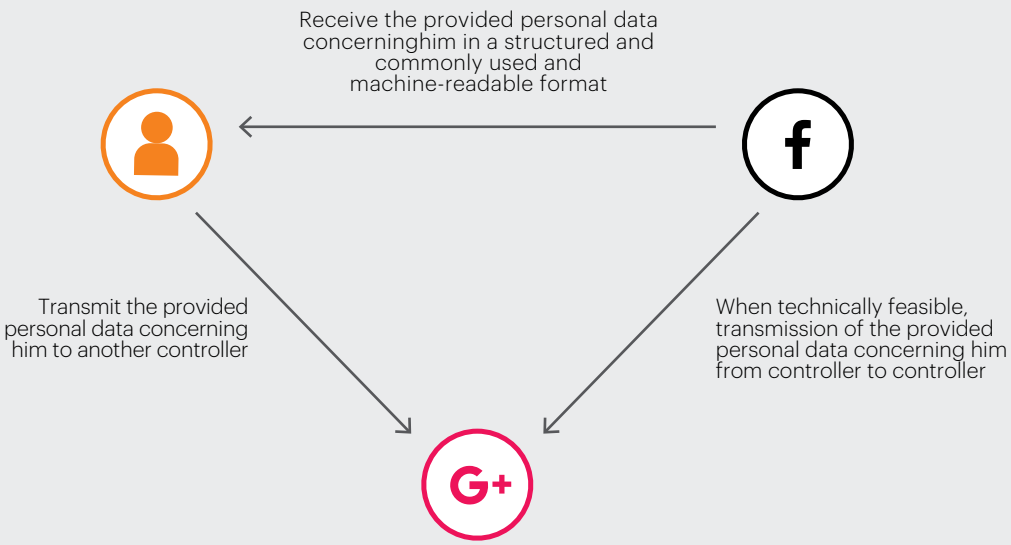
The GDPR includes other important changes vis-à-vis the Data Protection Directive, as summarised below:

Extension of the geographical scope

The current data protection rules only apply to controllers (i.e. those operators who determine the purposes and means of the processing of personal data (e.g. a credit institution)) with an establishment in the EU[114].

However, the GDPR will also apply to those controllers and processors (i.e. those operators who process personal data on behalf of a controller (e.g. a cloud service provider entrusted by a credit institution to store the personal data of its clients)) not established in the EU that:

FIGURE 9
Right to data portability of a social network user under the future GDPR (Cullen International)



— offer goods or services to individuals in the EU; or

— monitor their behaviour (e.g. profiling)[115].

Controllers and processors not established in the EU but subject to the GDPR will have to designate a representative in the EU, unless they process personal data occasionally and without a risk for the individuals[116].

New right to data portability

The GDPR introduces a new right to data portability[117]. Individuals will have the right to receive the personal data concerning them and which they provided to the controller and transmit it to another controller.

Further, when *"technically feasible"*, individuals will also have the right to transmission of the data concerning them from controller to controller.

Strengthened obligations for companies

Under the GDPR, the security obligations for controllers and processors will often depend on the level of risk that their processing operations generate[118]. Thus, the more risks a data processing operation entails for the individuals, the more security measures will have to be taken. Security measures include encryption or pseudonymisation.

In this context, controllers and processors will have to consider the risks presented in their processing operations, including the loss and unauthorised

TABLE 7
Obligations on companies (Cullen International)

Issue	Obligation
Data protection by design and by default [a/]	Controllers will have to implement data protection safeguards from the earliest stage of development of their products and services. They will also have to ensure that, by default, only the personal data which is necessary for each specific purpose of the processing is processed.
Data protection officer (DPO) [b/]	Controllers and processors will have to designate a DPO when they regularly monitor individuals on a large scale and when they process sensitive data (e.g. health data) on a large scale. Public authorities will always have to designate a DPO.
Data breach notification [c/]	Controllers will have to notify without undue delay data breaches to data protection authorities. However, they will not have to notify breaches which are not likely to result in a risk for the individuals.
Data protection impact assessment (DPIA) [d/]	Prior to a processing operation which is likely to result in a high risk for the individuals, controllers will have to carry out an assessment of the impact of that processing operation on the protection of personal data. For instance, DPIAs will be required before undertaking profiling and before processing sensitive data on a large scale.

a/ Article 25 GDPR; b/ Article 37 GDPR; c/ Article 33 GDPR; d/ Article 35 GDPR

disclosure of personal data. These risks may lead to a damage for the individual.

The table below summarises the obligations companies will have to comply with.

Companies will be able to demonstrate that they comply with their obligations by adhering to certifications, data protection seals and marks, and codes of conduct[119].

High fines in case of infringements

Under the current framework, it is up to Member States to set the fines for data protection infringements[120]. In this context, Member States have set low fines (e.g. the maximum fine foreseen in the UK is €0.69m[121])

However, fines in the GDPR range between up to €10m or up to 2% of the total worldwide annual turnover, whichever is higher, and up to €20m or up to 4% of the total worldwide annual turnover, whichever is higher, depending on the infringement[122].

For example, maximum fines could apply for infringements of provisions regarding the basic principles of the GDPR (e.g. conditions for consent) and the individual's rights (e.g. data portability).

DATA PROTECTION AUTHORITIES

Currently, online companies that offer their services in more than one EU country are being supervised by different national DPAs (i.e. the competent national DPAs in each EU country where they offer their services).

In this context, in recent years some national DPAs have launched cases in parallel against online companies that operate transnationally. For instance, the Spanish DPA imposed fines on Google that amounted to over €0.9m for seriously infringing data protection rights through its 2012 privacy policy[123].

One stop shop mechanism

One of the main changes introduced by the General Data Protection Regulation (GDPR) is the introduction of a one stop shop mechanism[124].

This implies that the DPA of the country of main establishment (i.e. the place of the central administration in the EU) of the controller or processor (e.g. the Irish DPA in the case of Google and Facebook) will be its sole interlocutor.

However, before adopting a measure that has a cross-border effect (e.g. an infringement of the GDPR affecting individuals in several Member States), the DPA of the country of main establishment (i.e. the lead DPA) will have to communicate the draft measure to the other concerned DPAs (i.e. the DPAs where the controller or processor has other establishments or the individuals affected by the processing reside)[125].

If any concerned DPA expresses an objection to the draft measure, the European Data Protection Board (EDPB) will have to make a final decision on the case[126].

The EDPB will be a new EU body with legal personality and composed of the heads of national DPAs[127].

Strengthening DPAs' independence and powers

Along with the introduction of the one stop shop mechanism, the GDPR will oblige EU countries to make sure that their DPAs *"remain free from external influence, whether direct or indirect and neither seek nor take instructions from anybody."*[128]

Further, under the GDPR DPAs will have the power to access the premises of controllers and processors, including their data processing equipment, in the course of their investigations[129].

CYBERSECURITY

The Budapest Convention is the only binding multilateral treaty instrument aimed at combating cybercrime. It was drafted by the Council of Europe in 2001[130]. The Convention provides a framework for international cooperation between state parties to the treaty, and is open for ratification also to states that are not members of the Council of Europe.

As for Latin American countries, to date only Panama and the Dominican Republic are part of the Convention. The Convention is the only substantive multilateral agreement with a stated objective of addressing cybercrime with convergent, harmonised legislation and capability building.

The Budapest Convention broadly attempts to cover crimes of illegal access, interference and interception of data and system networks, and the criminal misuse of devices. Additionally, offences perpetrated by means of computer systems such as computer-related fraud, production, distribution and transmission of child pornography and copyright offences are addressed by provisions of the Convention.

A United Nations resolution of December 2013[131] deals with the creation of a global culture of cybersecurity and the protection of critical information infrastructures. It recognises the growing reliance on information infrastructures by critical national services in areas such as energy, transport, financial services and public health.

Thus, the resolution invites UN Member States to develop strategies for reducing risks to critical information infrastructures, in accordance with national laws and regulations.

The ITU published in September 2011 a national cybersecurity strategy guide, setting main

initiatives to deploy, including a legal framework for cybersecurity, definition of authorities for coordinating, leading and managing responses to cyber threats and raising awareness in the population and in business[132].

EU POLICY AND REGULATORY INITIATIVES

The main actions taken by the EU with regard to cybersecurity are to:

— require all companies that process personal data to report personal data breaches, as referred to above in relation to the GDPR;

— require companies operating in certain vital sectors to protect their network and information systems and to report other types of significant cybersecurity breaches not involving personal data;

— raise the cybersecurity capabilities of the EU Member States and cooperation between them; and

— support the European cybersecurity industry in order to lessen Europe's dependence on non-EU vendors of ICT security products, services and software.

The EU has also set up two bodies with tasks related to cybersecurity and cybercrime:

— the EU Agency for Network and Information Security (ENISA)[133] to provide recommendations on cybersecurity and support EU policy development and its implementation; and

— the European Cybercrime Centre (EC3)[134] within Europol to coordinate cross-border law enforcement activities against cybercrime and act as a centre of technological expertise.

CYBERSECURITY REQUIREMENTS FOR COMPANIES OPERATING IN VITAL SECTORS

The EU adopted on 6 July 2016 its first legislation on cybersecurity: the Network and Information Security (NIS) Directive[135].

Following its publication in the EU Official Journal, in August 2016, EU Member States will have 21 months to transpose the directive into their national laws.

The NIS Directive was a key part of the European Commission's Cybersecurity Strategy of 2013[136].

The directive aims at ensuring a high common level of cybersecurity in the EU, and will cover companies providing the following types of services considered to be vital to the economy and society.

These companies will be required to protect their network and information systems and to report other types of significant cybersecurity breaches not involving personal data.

Currently at EU level there is only a requirement for telecommunications operators to report network security breaches.

RAISING THE CYBERSECURITY CAPABILITIES OF EU MEMBER STATES

The NIS Directive also aims to bring cybersecurity capabilities to the same level of development in all the EU Member States. Each Member State will be required to:

— designate a competent national authority for NIS and a Computer Security Incident Response Team (CSIRT); and

TABLE 8
NIS Directive - Scope of services covered (Cullen International)

'Essential services'	'Digital services'
— Energy (electricity, oil, gas) — Transport (air, rail, water, road) — Banking — Financial market infrastructures — Health sector — Drinking water supply and distribution — Digital infrastructure (internet exchange points, domain name system service providers, Top Level Domain name registries)	— Online marketplaces — Search engines — Cloud computing services

TABLE 9
EU cybersecurity groups (Cullen International)

	Cooperation Group	CSIRTs Network
Members	— EU Member States — European Commission — European Network and Information Security Agency (ENISA)	— National Computer Security Incident Response Teams (CSIRTs) — CERT-EU — European Commission (observer)
Role	Facilitate strategic cooperation and the exchange of information among Member States. Focused on exchange of best practices and capacity building. No role in coordinating responses to incidents, which will be done by the CSIRTs Network.	Promote swift and effective operational cooperation on specific cybersecurity incidents and sharing information about risks.
Secretariat	European Commission	ENISA

— set out a national cybersecurity strategy.

These requirements are intended to address the concern that currently Member States are at different levels of preparedness for dealing with cyber threats.

Two new EU groups will also be established to facilitate cooperation between Member States at strategic and operational levels respectively. These groups are expected to start work at the end of 2016 (six months after the adoption of the NIS Directive).

SUPPORTING THE EUROPEAN CYBERSECURITY INDUSTRY

The European Commission has announced, as part of its Digital Single Market strategy, plans to establish in 2016 a Public-Private Partnership (PPP) on cybersecurity[137].

The PPP is intended to address concerns that the European market for ICT security products,

services and software is dominated by non-EU global vendors.

The PPP will be a contractual arrangement between the Commission and *"an industrial grouping"*.

Its aim will be to stimulate Europe's cybersecurity industry by supporting research and development activities. Financial support will come from the EU Horizon 2020 research and development programme (H2020 includes €500m for cybersecurity and privacy between 2014-2020).

It is expected that the Commission will adopt in June 2016 a decision establishing the PPP and possibly a communication setting out additional policy measures (in areas such as certification, standardisation, labelling) that could help the European cybersecurity industry to grow.

4 —
NEW REGULATORY DEBATES

BIG DATA

Big Data could be defined as high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making, and process automation[138].

Consumers in the information society generate, every day, an inestimable amount of data.

The generation and use of data streams is useful for the improvement of government services. It is also essential for the development of different sectors (e.g. farming, automotive, retail, logistics, public administration). For instance, the use of big data analytics can considerably reduce manufacturing costs of companies.

According to the European Commission, the big data sector is growing 40% per year, seven times faster than the IT market as a whole[139]. Some estimations predict that big data could unleash €12tn in market value.

However, the use of big data within the EU is still low, and only one of the top 20 big data companies globally is European[140].

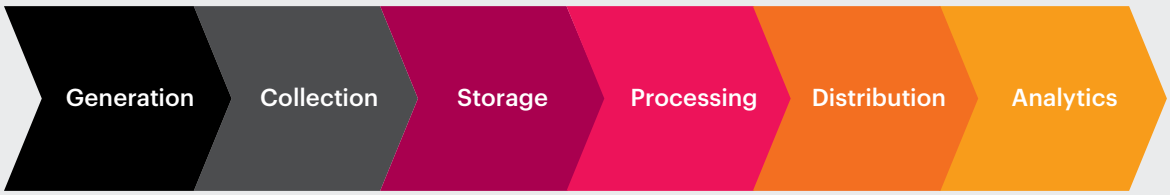
EU POLICY AND REGULATORY ISSUES

The European Commission published on July 2, 2014 a communication entitled *Towards a thriving data-driven economy*[141].

The Commission paper outlined a number of actions to be taken primarily by the Commission under four broad headings as shown in the chart below. Only a few of the proposed actions are regulatory and they fall mostly under the trust and security heading.

On the regulatory side, the most recent development with an impact on big data is the adoption of the General Data Protection Regulation (GDPR), which was described by the Commission as the regulatory backbone for the data driven economy.

FIGURE 10
The data value chain (OECD) [a/]



a/ Exploring data-driven innovation as a new source of growth, Mapping the issues raised by "Big Data", OECD, 2013, page 7 - http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP(2012)9/FINAL&docLanguage=En

FIGURE 11
Relevance of Big Data (source: European Commission)

4 STEPS TO LEVERAGE THE POTENCIAL OF BIG DATA

1. INVESTING IN IDEAS

Search for **game-shifting** ideas
Public Private Partnership
Research in Horizon2020

2. INFRASTRUCTURE FOR A DATA-DRIVEN ECONOMY

Network of data processing facilities
Invest in the Géant network
Supercomputing **centres of excelllence**
Build big data mobile internet through **5G PPP**
Telecoms Single Market for broadband investment

3. DEVELOP BUILDING BLOCKS

Guidelines on standard licences, datasets & charging
One-stop-shop to open data across the EU
Mapping big data standards
Open data i**ncubator fos SMEs**
Training for data professionals
Data market **monitoring** tool

4. TRUST AND SECURITY

EU **Data protection** rules
Guidelines on secure data storage
Consultation on:
- Policy ptions after Trusted Cloud Europe report
- Data ownership & liability of data provision
- User-controlled cloud-based technologies

In particular, the GDPR contains the purpose limitation principle, which implies that when personal data has been collected for one or various purposes, it should not be further processed in a way that is incompatible with the original purposes.

This, according to the Commission[142], does not prohibit the processing of personal data for the purpose of big data analytics. For example, in the case of traffic management systems, raw data can be used to analyse traffic flows in order to reduce congestion. In this context, the use of pseudonymisation and encryption techniques, which are both foreseen in the GDPR, play a key role.

FORTHCOMING REGULATORY INITIATIVES

Furthermore, as part of its free flow of data initiative, which is expected in November 2016, the Commission will tackle emerging issues with an impact on the development of big data technologies. These issues include data ownership, interoperability, usability and access to data, as well as liability issues[143]. However, the concrete content of the proposal is still uncertain.

CLOUD SERVICES

Cloud computing means **storing and accessing data and programs over the internet** instead of on the hard drive of a device or on a home or office network.

For some types of cloud services, data and programs may still be stored locally on the device, but **synchronisation** allows all of the user's devices to access the same data.

Common examples of cloud-based services used by **individual consumers** include: **webmail** (e.g. Gmail), **online storage and synchronisation** (e.g. Apple iCloud), and **social media** (e.g. Facebook). Cloud services offered to individual consumers are often **free to use**, although **personal data** may be collected to serve **targeted advertising** to the user or for other purposes.

USE OF CLOUD SERVICES IN THE EU

The take-up of cloud computing services in the EU is still relatively low: 19% of EU businesses bought cloud services in 2014, and 30% of private internet users used cloud storage in 2015[144].

The total value of the cloud market for the EU in 2013 was estimated at €9.5bn, less than 3% of the overall IT budget of the public and private sector in the EU[145]. This value is expected to grow to €44.8bn by 2020, accounting for over 10% of the forecasted IT budget in 2020.

The main aims of the EU with regard to cloud computing are to increase trust in cloud services and to remove barriers to the cross-border

provision of cloud services across the single market.

The European Commission has announced, as part of its Digital Single Market strategy, plans to take action in 2016 in several areas related to cloud computing.

A Free Flow of Data initiative will address unjustified restrictions on the location of data for storage or processing purposes that hinder the provision of cloud services[146].

A European Cloud initiative will also aim to create trust in cloud computing, including:

— certification;

— contracts; and

— switching of cloud services providers[147].

Previously, the Commission set out in 2012 a European Cloud Strategy[148]. A central part of this strategy was the establishment of the Cloud Select Industry Group (C-SIG)[149] to develop industry self-regulatory guidelines in relation to:

— Standardisation guidelines for Service Level Agreements between cloud providers and corporate cloud users that were published in June 2014[150].

— A code of conduct on data protection by cloud service providers[151].

Several pieces of more general EU legislation such as the General Data Protection Regulation are also particularly relevant to the provision of cloud computing services.

In particular, the Network and Information Security (NIS) Directive[152] will require providers of cloud computing services to take appropriate cybersecurity measures and to notify significant security breaches (complementing the requirement in the GDPR to notify personal data breaches).

Furthermore, a requirement for the retrieval of digital content is included in the Commission Proposal for a Directive on contracts for the supply of digital content.

In particular, in the case of termination of a B2C contract (e.g. cloud storage), the supplier would have to provide the consumer with the technical means to retrieve all the consumer's content and data produced/generated through the use of the digital content[153].

INTERNET OF THINGS

The IoT is understood as an ecosystem where different objects connect among themselves and applications. It has been developed in areas such as manufacturing, transport, healthcare, devices), helping them to relate to each other.

The number of Internet of Things (IoT) connections within the EU is estimated to increase from 1.8m in 2013 to 6bn in 2012, while the value of the EU IoT is expected to exceed €1tn by 2020[154].

EU POLICIES AND REGULATORY INITIATIVES ON IOT

At present, in the EU there is no specific regulation targeting the IoT. The European Commission is of the view that the IoT can flourish in Europe through open platforms and joint standardisation efforts, as well as a supportive legal framework covering areas such as privacy, security, spectrum and roaming.

As stated above, the Commission announced in its DSM strategy that it will deliver the free flow of data initiative. Along with data localisation requirements, this initiative is expected to specifically address some IoT related issues.

In particular, this initiative will address emerging issues in relation to data ownership, access and liability that are important for the roll-out of the IoT[155].

The European Commission published on 19 April 2016 a staff working document on the IoT[156]. In order to make Europe a leading region in IoT products and services, the document sets out a number of issues that have to be addressed, as summarised in the table below.

In the communication on ICT standardisation priorities, the Commission has identified the IoT as one of the five priority areas for industry and standardisation bodies to work on[157].

The Commission plans to favour open platforms for IoT that can be used across different IoT applications. The EU-supported FIWARE[158] is mentioned as an example of an open platform.

In addition, Commission is funding large scale IoT pilots[159] under the Horizon 2020 research and development programme covering:

TABLE 10
IoT issues to be addressed (European Commission)

Pillar	A single market for IoT	A thriving IoT ecosystem	A human-centred IoT
Principle	IoT devices and services should be able to connect seamlessly and on a plug-and-play basis anywhere in the EU, and scale up across borders.	Open platforms that can be used across IoT applications should be promoted as these will help developer communities to innovate.	The IoT in Europe should be based on European values, notably high standards for the protection of personal data and security.
Policy/ regulatory response	— Standardisation and interoperability — Free flow of data initiative	— Promoting open platforms — EU-funded large scale IoT pilots	— Privacy

— smart living environments for ageing well;

— smart farming and food security;

— wearables;

— smart cities; and

— driverless cars.

ENABLING IOT: BEREC'S PERSPECTIVE

BEREC, the European regulators group, identified some future work items but did not report any new substantive issues in its report 'Enabling the Internet of Things' published in February 2016[160]. The reports will serve as BEREC's input for the European Commission's review of the EU regulatory framework for electronic communications.

BEREC points out that, in order for IoT services to thrive, several pre-conditions need to be fulfilled:

— sufficient resources (i.e. spectrum and identifiers);

— a regulatory framework fit for IoT services; and

— acceptance of IoT services by consumers (i.e. resolving privacy, security and interoperability issues).

According to BEREC, it should be assessed (within the ongoing regulatory framework review) whether and, if so, to what extent the existing rules, which were primarily designed for voice telephony, are also fit for M2M communications. BEREC considers that, in general, no special treatment of IoT services and/or M2M communications is necessary, except in the following areas:

— roaming (case by case analysis required);

— switching, co-existence of both MNC (mobile network code) assignment and OTA (over the air) SIM provisioning with a need for flexibility at the national level; and

— number portability, a new approach taking into account the nature of IoT services.[161]

According to BEREC, there is no need for a European numbering scheme for M2M communications, since the use of existing resources (extraterritorial use of numbers and the use of ITU numbers) should be sufficient for the time being.

On data protection, BEREC would prefer a careful evolution of the existing EU rules to adapt them to the IoT environment (e.g. rules on information and consent should be made as user-friendly as possible). BEREC considers the Council general approach of 15 June 2015 regarding the Commission proposal for a General Data Protection Regulation as a step in the right direction.

SHARING ECONOMY

OVERVIEW IN THE EU

The collaborative consumption notion is a new trend where users move from ownership rights to access rights. Nowadays, entire communities are sharing, lending, gifting, renting, and swapping services through online platforms, in areas such as transport, travel, retail, home services, real estate and accommodation.

As a part of the Digital Single Market (DSM) strategy, the European Commission has been studying the regulatory environment for platforms and in particular, for those used in the collaborative economy.

The European Commission is not planning EU regulation specifically targeting the collaborative economy and hence providers such as Uber and Airbnb.

In June 2016 the Commission delivered a non-binding communication[162] aimed at guiding both Member States and operators on how existing EU legislation applies to the collaborative economy. Member States remain free to decide on the way they approach the collaborative economy, as long as they comply with EU law[163].

The communication can also help predict how the European Commission is going to interpret and apply EU law when it is confronted with specific cases (e.g. a collaborative economy platform sends a complaint to the Commission against a Member State whose legislation does not allow the provision of its services).

The communication notes that the collaborative economy involves three types of actors:

— Service providers (e.g. a person who offers an apartment for short-term rental use), who can be a private individual that offers services on an occasional basis (i.e. a peer) or a service provider who acts in his professional capacity (i.e. a professional service provider)

— Users (e.g. a tourist)

— Intermediaries connecting, by means of an online platform, service providers with users and facilitating transactions between them (e.g. Airbnb).

The Commission's communication also makes a distinction on market access requirements, i.e. referring to authorisations, licences or other requirements that national authorities can impose on service providers to provide a collaborative service. In particular, the Commission makes a distinction between professional providers (B2C), peer-to-peer providers (C2C), and online platforms only providing an information society service and not the underlying service as well. According to the Commission, only professional services should be subject to market access requirements, and Member States should review their existing laws "to ensure that market access requirements continue to be justified by a legitimate objective."

According to the Commission, *Member States should take into account the specific features of collaborative economy business models, and banning an activity* or imposing quantitative restrictions (e.g. limiting the number of licences) should be measures "of last resort."

Although very popular among consumers, these new platforms are criticised by conventional market players for the different (lighter) regulatory and fiscal obligations applicable to them.

There has been much debate around some of these platforms. For example, court decisions in Belgium, Italy, France, Germany, Spain and in other countries

worldwide, have banned UberPOP (peer to peer transport).

Some governments are studying the impact of peer-to-peer (P2P) markets and are trying to understand how to introduce consumer, taxation or competition rules to the sharing economy, without limiting the sector's development and innovation.

5 —
IMPLEMENTATION OF THE EU DSM STRATEGY: OVERVIEW AND STATUS

In terms of implementation, an overview of the main steps taken in each of the three pillars and 16 actions identified in the DSM strategy, is summarised in the tables below.

TABLE 11
Implementation of Pillar 1 (Better access for consumers and businesses to online goods and services across Europe)

Topic	Action	Timing	Status June 2016
Contract rules for cross-border e-commerce	Amended legislative proposal to replace the withdrawn proposal for a Common European Sales Law. The proposal will: — cover "harmonised EU rules for online purchases of digital content"; and — *"allow traders to rely on their national laws based on a focused set of key mandatory EU contractual rights for domestic and cross-border online sales of tangible goods".*	Before end of 2015	No consensus yet on proposal. No significant developments since 2015
Cooperation between consumer protection authorities	Review of the Consumer Protection Cooperation Regulation *"in order to develop more efficient cooperation mechanisms"* between national consumer protection authorities.	2016	May 2016: proposal for a new regulation on consumer protection cooperation (CPC) that will replace the existing 2004 CPC Regulation. Updated guidance on unfair commercial practices to respond in particular to risks presented by the digital world
Cross-border parcel delivery	*"Measures to improve price transparency and enhance regulatory oversight of [cross-border] parcel delivery"*. The measures were not specified.	First half of 2016	May 2016: draft regulation on cross-border parcel delivery services aimed at increasing the transparency of prices and improving regulatory oversight
Geo-blocking	Legislative proposals *"to end unjustified geo-blocking. Action could include targeted change to the e-Commerce Directive and the framework set out by article 20 of the Services Directive"*	First half of 2016	25 May 2016: draft regulation aimed at ending unjustified geo-blocking and other forms of discrimination on the grounds of nationality, residence or establishment
E-commerce sector inquiry	Launch of a competition sector inquiry focusing on contractual restrictions to cross-border e-commerce, such as geo-blocking.	2015	Launched in May 2015. Initial findings presented in March 2016

Continued on next page →

Topic	Action	Timing	Status June 2016
Copyright reform	Legislative proposals "*to reduce the differences between national copyright regimes and allow for wider online access to works by users across Europe, including through further harmonisation measures*". However, the Commission does not intend to challenge the territoriality principle. The proposals will include: — "portability of legally acquired content"; — "ensuring cross-border access to legally purchased online services"; — "greater legal certainty for the cross-border use of content for specific purposes" such as text and data mining "through harmonised exceptions"; — "clarifying the rules on the activities of intermediaries in relation to copyright-protected content"; and — "*modernising enforcement of intellectual property rights, focusing on commercial scale infringements*" (this last aim will be addressed separately in 2016).	Before end of 2015	Proposal presented May 2015. Agreement on general approach reached at Council in May 2016
Satellite and Cable Directive	Review of the Satellite and Cable Directive to "*assess the need to enlarge its scope to broadcasters' online transmissions*".	2015/2016	Review is ongoing
VAT	Legislative proposals to "reduce the administrative burden on businesses arising from different VAT regimes". The proposals will include extending the One-Stop Shop for VAT payments due on electronic services to online sales of tangible goods. The Commission will also "*explore how to address the tax treatment of certain e-services, such as digital books and online publications, in the context of the general VAT reform*".	2016	Action plan adopted in April 2016

TABLE 12
Implementation of Pillar 2 (Creating the right conditions for digital networks and services to flourish)

Topic	Action	Timing	Status June 2016
Reform of telecoms regulatory framework	Proposals *"for an ambitious overhaul of the telecoms regulatory framework"*. The proposals will focus on: — "a consistent single market approach to spectrum policy and management"; — "tackling regulatory fragmentation"; — "ensuring a level playing field for market players", traditional and new; — "incentivising investment in high speed networks"; and — *"a more effective regulatory institutional framework"*.	2016	No proposal presented yet (expected Oct. 2016)
Audiovisual Media Services Directive	Review the AVMS Directive, although no mention of presenting a legislative proposal. The Commission will re-assess the two-tier approach and "consider whether the current scope or the rules should be broadened to encompass new services and players that are currently not considered as audiovisual media services under the directive and/or providers that fall outside its current geographical scope". Assessment of existing rules will focus on measures to promote EU works on VOD platforms, advertising rules and rules on the protection of minors. The working document accompanying the communication also mentions independence of regulators and accessibility to content of public interest.	2016	Proposal presented in May 2016
Online platforms and intermediaries	*"Comprehensive assessment of the role of platforms, including in the sharing economy, and of online intermediaries"*. The assessment will cover issues such as: — *"transparency, e.g. in search results (involving paid-for links and/or advertisement)";* — *"platforms' usage of the information they collect";* — *"relations between platforms and suppliers";* — *"constraints on the ability of individuals and businesses to move from one platform to another"*. In parallel with its assessment of online platforms, the Commission will also *"analyse how best to tackle illegal content on the internet"*.	Before end of 2015	Communication published in May 2016. No regulation foreseen at the moment
e-Privacy Directive	Review of the e-Privacy Directive once the General Data Protection Regulation has been adopted.	2016	Data Protection Regulation published May 2016. Review of e-Privacy directive: public consultation launched April 2016 still ongoing
Cybersecurity	Launch of *"a public-private partnership on cybersecurity in the area of technologies and solutions for online network security"*.	First half of 2016	Public consultation and roadmap launched Dec. 2015. No new developments since

TABLE 13
Implementation of Pillar 3 (Maximising the growth potential of the European Digital Economy)

Topic	Action	Timing	Status June 2016
Interoperability and standardisation	Adoption of a "*Priority ICT Standards Plan*" to define key priorities for standardisation, including in the health, transport, environment and energy sectors.	2015	EC Communication published in April 2016.
Big data, cloud, Internet of Things	A "*European free flow of data initiative*" to tackle: — "restrictions on the free movement of data within the EU for reasons other than the protection of personal data"; — "unjustified restrictions on the location of data for storage or processing purposes"; — "emerging issues of data ownership" (e.g. in the context of the Internet of Things); and — "access to public data to help drive innovation". The Commission will also launch "*a European Cloud initiative including cloud services certification, contracts, switching of cloud services providers and a research open science cloud*". It was not explained how this would fit with existing initiatives under the Commission's 2012 Cloud Computing Strategy (Tracker).	2016	Working document on IoT published in April 2016 Publication on IoT and OTTs by BEREC in March 2016
E-government	E-government action plan for the period 2016-2020.	2016	Published in April 2016

PART II — LATIN AMERICA

6 —
LATIN AMERICAN TELECOMS: INFRASTRUCTURE CHALLENGES

With the exception of a few countries, Latin American telecommunications have long been liberalised, foreign ownership restrictions removed, and national regulatory authorities, implementing and supervising over the sector's regulation, have been established.

The telecoms sector has evolved in all countries since the 1990s, with a significant role played by mobile technologies, which triggered relevant infrastructure investment, bridged network coverage gaps in many countries and regions, and increased access by citizens.

In Latin America few options exist for entrants for access to third party fixed infrastructure on a regulated wholesale basis in order to compete in retail broadband markets. No significant new entries have been observed in Latin America's retail fixed broadband markets, where competition is mainly between incumbent telcos and cable operators. Where regulated wholesale unbundled access has been imposed in Latin America[164], it was done so over ten years after the EU's adoption of its local loop unbundling (LLU) regulation[165], raising doubts on the capacity of LLU to address new entrants' demand in a continuously evolving technology scenario.

FIXED BROADBAND

Fixed broadband take-up by Latin American households is less ubiquitous than in Europe, but coverage and take up have however increased over the last few years, as is shown in the figure below for 13 selected countries.

Uruguay is the country with the highest fixed broadband penetration rate, with 66% of households subscribing in 2015. In Argentina, Chile and Mexico residential fixed broadband penetration exceeds or is close to 50% of households. In 2015, fixed broadband penetration decreased by 2.5% in Chile, and remained stable in Argentina and Brazil. In Ecuador fixed broadband penetration reached 45% at end-2015, according to Arcotel data.

The figure below reports the breakdown by technology in selected countries, where such information is made available by regulators[166].

In terms of technologies, Uruguay is the only country among those monitored herein where DSL is by far the most significant technology, followed by Peru, Ecuador, and Argentina[167]. In Brazil, Chile, Colombia, Mexico and Costa Rica, competition among different platforms is observed, with a significant presence of cable networks in the most densely populated areas.

Fibre network access is observed in Mexico, Ecuador and Brazil, although still at very limited levels among residential users. In some countries, WiMax or other fixed-wireless access technologies have been used by new entrants. This is the case of alternative operator Axtel in Mexico, using wireless local loop technology to offer telephony and lower speed internet access as a (cheaper) alternative to deploying own access networks, before LLU was mandated by the regulator in Mexico.

FIGURE 12
Fixed broadband subscriptions as a percentage of households
(Cullen International based on national regulators' data)

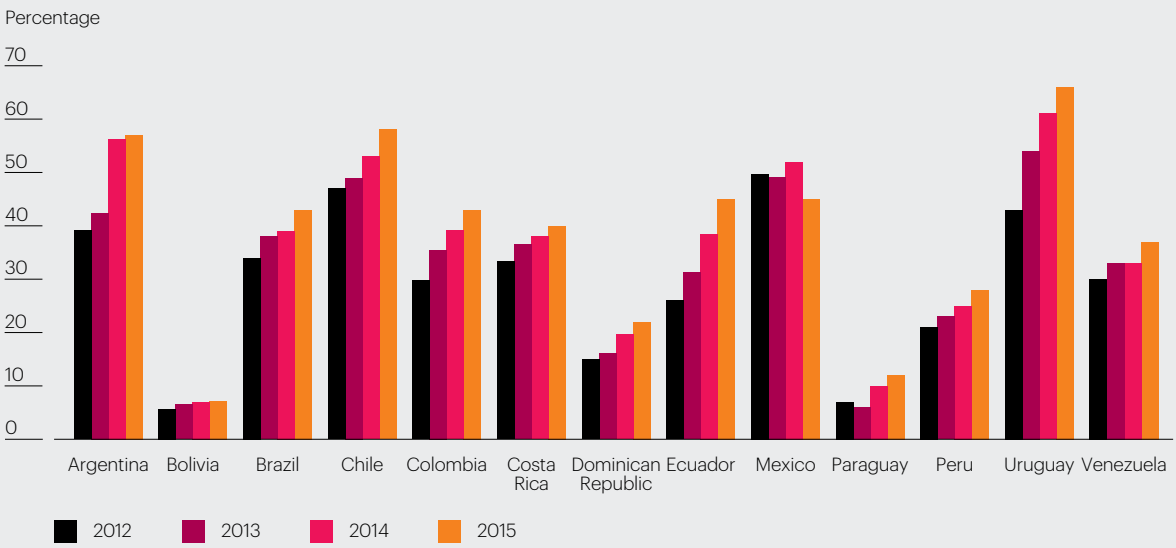
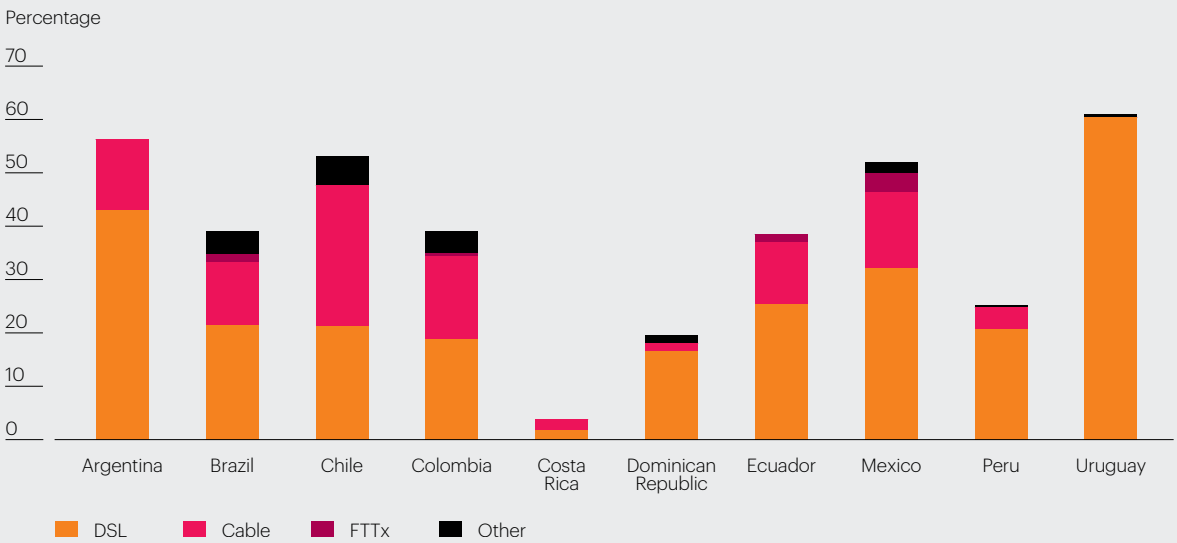


FIGURE 13
Fixed broadband household penetration and main technologies in use, 2014
(Cullen International based on national regulators' data)



Example 1 —
Fixed-wireless broadband in Brazil

In Brazil Sky and ON Telecom have been the first companies to start offering fixed-wireless, and this by use of spectrum in the 2.5 GHz band.

Sky (satellite pay TV provider owned by DirecTV) launched 2 Mbps and 4 Mbps internet services in Brasilia in 2011. The service targets residential customers, whether or not buying or willing to buy pay-TV from Sky, and is now available in large and medium size cities in 24 Brazilian states [a/].

ON Telecom operates in the São Paulo State and offers up to 10 Mbps wireless broadband with a monthly data cap mainly to residential users by use of the unpaired (TDD) 2.5 GHz spectrum band. The company launched fixed TD-LTE services in 2013 in the city of Itatiba. Three years later, the company was offering broadband services in 133 cities in the São Paulo State.[b/]

Building upon the potential of this business model to increase competition and broadband availability in small and medium cities of Brazil, in its multi-band spectrum auction of December 2015 Anatel also offered 60 MHz of unpaired TDD spectrum in the 2.5 GHz and 1900 MHz bands. This spectrum was licensed with local scope to small and medium companies, to enable fixed wireless broadband in 876 cities [c/].

a/ https://www.skybandalarga.com.br/#planos
b/ http://on.com.br/
c/ Auction 2/2015 rules: http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=19/04/2016&jornal=3&pagina=84&totalArquivos=212

More recently, new market entries based on new and faster fixed-wireless access technologies have been observed in selected countries in areas where high demand is combined with insufficient (or unsuitable for broadband) fixed network infrastructure.

MOBILE BROADBAND

Latin America is one of the world regions with the highest dynamism and take-up of mobile broadband. Take-up has been increasing substantially, and mobile network coverage and quality requirements are often imposed by national regulators whether as a spectrum licensing requirement, or under consumer protection regulations.

The high figures appearing in Costa Rica and in Brazil are partly explained by the very high penetration of mobile services, as well as by the adoption of

FIGURE 14
Mobile broadband subscriptions as a percentage of total mobile subscriptions
(Cullen International based on ITU data)

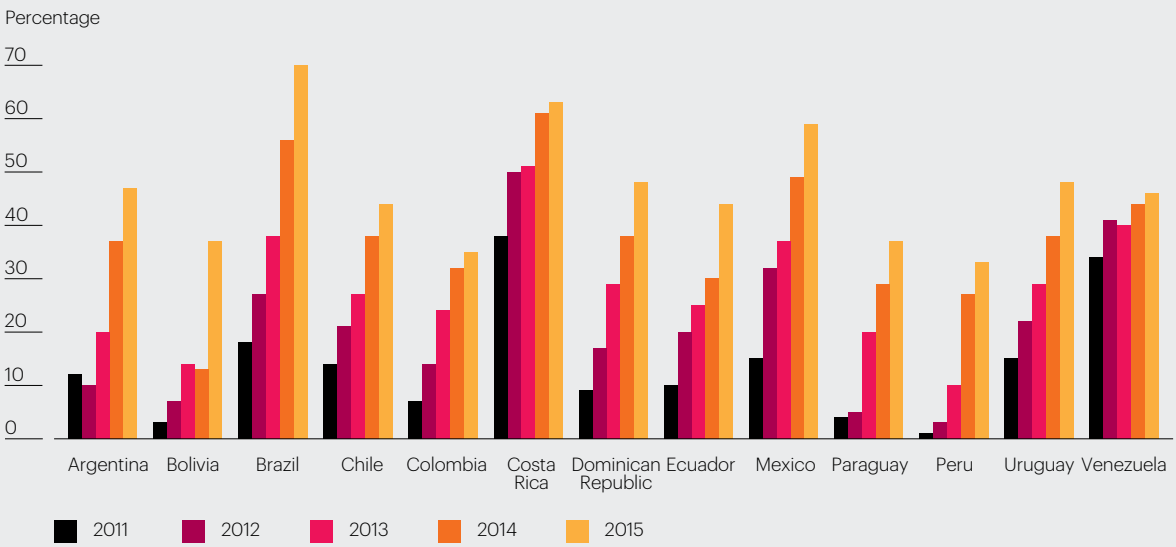
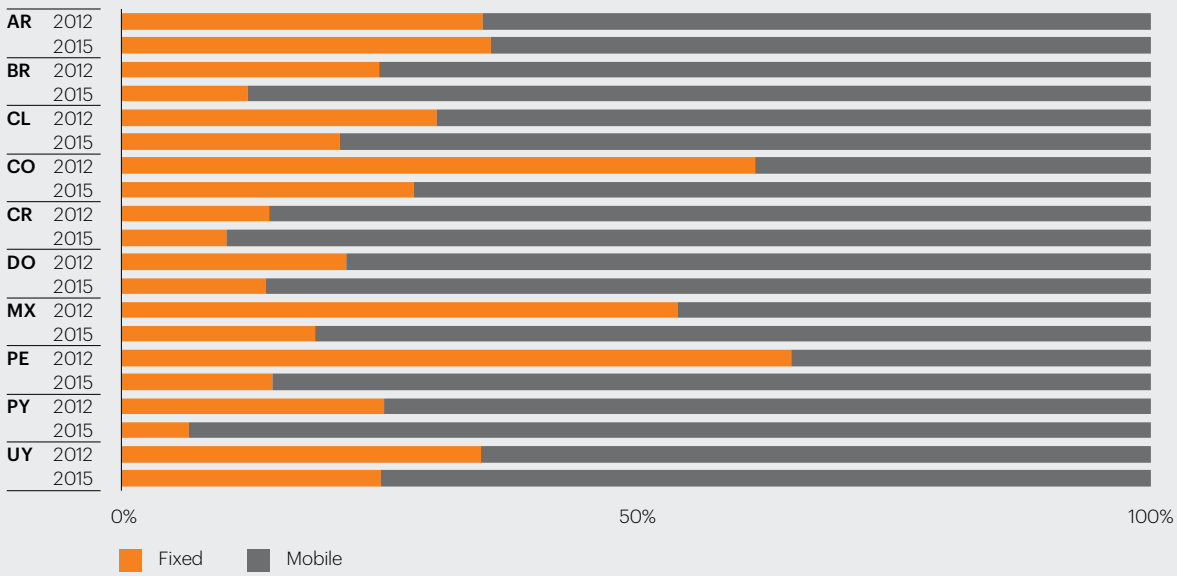


FIGURE 15
Mobile broadband subscriptions as a percentage of total mobile subscriptions
(Cullen International based on ITU data)



multiple SIM cards by individual users. In both countries more than 50% of active mobile service users are also mobile broadband users.

According to Anatel data, at end-2015 while total mobile subscribers decreased in Brazil from the previous year by 8.2% (from 280.7m to 257.8m) mobile internet users increased by 14.3%, from 157.9m to 180.5m. Brazil is also one of the top countries for use of OTT services and applications on mobile networks. According to official data by Facebook, 62m people (i.e. 45% of the Brazilian population) access Facebook at least once a day; of these, 50m access from a mobile handset[168].

Mobile broadband adoption shows growth trends in all countries. Mexico, Argentina, and Colombia show an impressive growth path over the past few years: in 2011 mobile broadband services were used by no more than 10% of all mobile service users in those countries.

The share of mobile broadband versus fixed broadband has been increasing substantially from 2012 to 2015, as is shown in the figure below.

NET NEUTRALITY DEBATE IN LATIN AMERICA

In Latin America there is no unified approach towards net neutrality.

Net neutrality has been mandated by law in seven countries, including in Argentina, Brazil, Chile, Colombia, Ecuador, Mexico and Peru. In Costa Rica net neutrality provisions are included in the National Broadband Strategy, and in Paraguay such provisions are included in telecommunication services regulation.

Comparing with the European approach, Chile is the only country setting similar regulations regarding transparency, blocking, charging extra for premium services and zero rating regulation.

A proposed regulation in Peru is also in line with the European approach, and takes a step further by requesting specific regulator's authorisation for each zero rating plan offered. The proposed rules focus on how Osiptel will address possible exemptions to the arbitrary conduct prohibited under the general net neutrality rules of 2012.

In Brazil, President Rousseff signed the implementing decree of the 2014 Internet Law ('Marco Civil') the day before the Senate's vote in favour of the impeachment procedure against the president. The decree provides more detail on the net neutrality rules applicable to broadband access, exempting specialised services from their scope. Users' rights to the protection of personal data are also further specified.

A working group on Net Neutrality, coordinated by the Chilean regulator Subtel is currently part of

Regulatel activities. A report on *"Neutralidad de la Red: Cambios Normativos y Eventos del Mercado"* was published in May 2016 as a first deliverable of the Regulatel working group. The report is not publicly available as of today.

INTERNATIONAL ROAMING IN LATIN AMERICA: CURRENT CHALLENGES

According to a study by GSMA (2013)[169], the low percentage of travellers on the total population of Latin America has traditionally represented a restriction to the possibilities for growth of the international roaming market in Latin America.

However, with the growth of trade and tourism, more roaming routes have become economically viable, allowing an increase in the supply, and a growth of the roaming market.

According to the same study, between 4% and 5% of the Latin American population lives in border areas, and mobile operators in the region have been working on the solution to problems related to inadvertent roaming in border areas (i.e. when the customer captures the neighbouring country's operator signal and, without wanting it or requiring it, uses its roaming service while in the home country). The solutions include both commercial and technical measures.

The mobile industry in Latin America and the Caribbean has also been introducing mechanisms to improve the pricing and billing of roaming to customers, including monthly plan offers that include roaming minutes, billing communications based on the final price, prepaid roaming, unified or flat rates and prevention of Bill Shock.

The industry has been working on implementing standard rates in each country and will possibly,

once that process is completed, start considering more homogenous prices across the region.

However, one of the main problems identified by industry is taxation. Tax rules are divergent throughout Latin America and this becomes a substantial burden on roaming pricing.

Taxes are a significant proportion of the cost of the service due to high taxation itself in certain countries, and to double taxation. This has negative impacts on the profitability of usage plans, and limits the possibilities for innovation and reducing the pricing offer.

Recent studies estimate that 72% of roaming routes in Latin America are subject to double taxation[170].

The Chilean, Mexican and Colombian regulators recently announced[171] their intention to share information and jointly analyse the convenience of regulating international roaming in Latin America. A similar initiative was announced in 2014, when the governments of Chile and Argentina signed a political agreement to cooperate on international roaming regulation and make progress in the creation of a bilateral interconnection network[172].

Concrete results were recently reached in Mexico, where international roaming charges with the US were eliminated from 2016. It should be noted however that the elimination of roaming charges between Mexico and the US was decided by mobile operators —therefore representing a market-led decision rather than a legal or regulatory obligation imposed by regulatory authorities.

ADDRESSING INFRASTRUCTURE FRAGMENTATION IN LATIN AMERICA

If infrastructure fragmentation is still an issue in the EU, it is certainly so, and to a much higher degree, in Latin America. The great extension of the region, is combined with the presence within it of very large individual countries, such as Brazil or Mexico, as well as of very small countries, especially in Central America and the Caribbean.

The sector is characterised by the presence (much smaller compared with Europe) of legacy infrastructure. Policies and regulations, including spectrum management, are always defined at national level.

Differences across countries are seen at different levels: each country has its own institutional environment, with the national government setting policies and priorities, and a national regulatory authority implementing and enforcing the national framework. Differences concern all aspects of regulation, including licensing regimes, universal service regimes, pricing regimes, consumer protection regimes, as well as the competition framework, network interconnection and access regimes, the way spectrum is allocated and assigned, and so on.

Regulatory environments across the region are far from achieving the technology and service neutrality that the current internet world would demand. The public debate on net neutrality, privacy and data protection, as well on the impact of OTT players in the market is often characterised by very opposing fronts, unable to find solutions that may be suitable for industry and society at large.

However, similarities can also be identified at regional level.

The region lacks networks infrastructure: this is observed in almost all Latin American countries. Economic instability, and risks related to regulatory and market development uncertainties are considerable barriers to the uptake of the required private investment in many countries. The political and economic climate can have a significant impact over investment decisions, especially if these come from foreign investors.

As in Europe, some players operate in multiple countries across the region. This is certainly true for the two very large, 'historic' investors in Latin America, like Telefonica and América Móvil. However other groups, have recently increased their presence in Latin America over the past few years, for instance AT&T, Millicom, Liberty Global, and Digicel.

Business models, services offered, and regional presence (as in the case of the players in Central America and Caribbean territories) vary. But what all the foreign investors have in common is the need to ensure adequate return on their investment.

Some countries over the past few years have engaged in new debates and initiatives aiming at bridging the significant infrastructure gaps and contributing to internet service affordability across the region.

For example the *Red de Conectividad Suramericana para la Integración* (South American Connectivity Network for Integration) is an initiative promoted by the Union of South American Nations (UNASUR)[173]. The initiative aims for the creation of a fibre-optic backbone network exclusively financed by Latin American institutions.

According to UNASUR, the creation of the proposed network could reduce South America's reliance on foreign businesses for the infrastructure needed to connect to the Internet, subsequently lowering costs of access as well as increasing connectivity speeds[174].

SPECTRUM HARMONISATION IN LATIN AMERICA

Latin America's situation differs from that of Europe, as there is no regional body issuing binding decisions on spectrum harmonisation. Spectrum allocation remains a national matter subject to recommendations from international and regional organisations such as the ITU and CITEL.

In the Americas region, spectrum harmonisation powers are mainly concentrated in CITEL. CITEL is the organisation in charge of transposing WRC decisions into the region. Although its decisions are not binding, CITEL is where the regional debate between Member States and industry takes place.

The CITEL strategic plan has two main objectives related to spectrum:

— fostering and supporting the transition to digital broadcasting and the efficient use of the digital dividend spectrum

— promoting efficient and equitable use of spectrum in the region on the basis of studies and technological advances according to the priorities and requirements of the Member States.

All of these spectrum issues are dealt with by the permanent consultative committee II (PCC-II), including the development of common positions and preparation of the Inter-American proposals on the radio communications topics planned for the world and regional conferences of the ITU. PCC-II has four study groups, respectively dealing with radio communications conference preparations and spectrum issues of terrestrial, satellite and broadcasting services.

IDENTIFYING KEY ELEMENTS OF A SINGLE TELECOMMU-NICATIONS MARKET IN LATIN AMERICA

In the EU, despite the presence of a common Policy and Regulatory Framework for electronic communications, a single telecommunications single market is still under construction.

In terms of infrastructure and connectivity, it is unlikely that the 2020 Digital Agenda targets will be achieved in every EU Member State. As we have seen in the previous chapters, there are still differences across the EU in terms of fast broadband coverage and penetration, or in terms of digital literacy.

Despite the presence of several groups operating in multiple EU countries, network infrastructure continues to be operated and exploited at national level, and the related inputs and resources, such as radio spectrum, are administered by national regulatory authorities.

However, even in this far-from-perfect scenario, the EU and Latin America differ in many respects.

TABLE 14
Main differences between EU and Latin American 'elements' of a single market

Element	EU	Latin America
Institutional framework	Member States are bound to EU Treaties, regulations and directives. Recommendations and guidelines are non-binding, but non-compliance must be justified. Enforcement can scale-up to the Court of Justice of the EU.	No unified and binding institutional framework encompassing all Latin American countries. Some sub-regional trade agreements involve some of the countries, for example Nafta and Mercosur.
Authorities	Regulators in each Member State must be independent, to ensure the impartial implementation of the EU rules, so as to ensure free competition and that there is no discrimination against other EU Member States' businesses and consumers. Role of BEREC for the harmonised implementation of competitive rules.	Each country has national regulatory authority (NRA). Level of independence from government may vary as well as the responsibilities and functioning of each NRA. Multilateral organisations such as Regulatel, play an advisory and exchange role in the regional regulatory debate.
Spectrum harmonisation	Role of the RSPG for spectrum harmonisation	CITEL is in charge of transposing WRC decisions into the region.
Broadband plans	Each Member State has adopted its own broadband plan, reflecting national circumstances. However, there is a common digital agenda at EU level with (non-binding) targets, and a strategy for the digital single market. Legislative and other binding EU instruments aim towards the achievement of the strategies defined for the whole EU	Countries adopt own broadband plans, reflecting national circumstances. No coordinated efforts or common targets for the region.
Competition	Member States must comply with the competition requirements set forth at EU level, to avoid any detrimental impact on the internal market, and not to distort competition within the EU. Many rules are defined by Member States, but in accordance with the procedures and Guidelines set forth at EU level. Possibility for the EC to intervene in individual states' market analyses. Advisory role of the BEREC.	Fragmented scenario, with only some of the NRAs implementing market analyses and related remedies on operators having Significant Market Power. No common methodology or best practices. Wholesale regulation or competitive safeguards for new entrants are unevenly observed (or have been introduced only very recently) in Latin America.

7 —

ACCESS TO ONLINE DIGITAL GOODS AND SERVICES IN LATIN AMERICA

E-COMMERCE IN LATIN AMERICA

A study by CEPAL/Fundación Telefónica (Katz, 2015)[175] shows that Latin America has reached an advanced level of adoption of digital technologies when compared to other emerging regions, despite 50% of its population not yet using the Internet. In 2013, the region had an Internet penetration superior to the world-average, also surpassing Asia-Pacific, Middle East and Africa. The amount of hours spent online by users from some countries in the region approaches the world-average, whereas a stronger presence is found when online social media activities are considered.[176]

When it comes to e-Commerce, the same study estimated that revenues generated by online platforms in the region reached US$9,242m (2013)[177], including revenues generated by local or global online retailers operating in the region, as well as revenues generated by Taringa, a social media platform launched in Argentina, with presence in Chile, Mexico and Uruguay.

According to market research by PayPal (2014)[178], if we also consider the value of the products traded online, the total turnover of e-Commerce in selected Latin American countries (Argentina, Brazil, Chile, Colombia, Mexico and Peru) will account for US$100bn in 2018, a growth of 177% in relation to 2014. According to the study:

— The growth of e-commerce in the region is explained by an increasing level of consumer confidence in payment methods and broader connectivity.

— Brazil, Mexico and Chile are the countries where consumers will spend more money on online shopping by 2018, potentially surpassing the average of the US consumer.

— To date, Brazil shows the highest rate of e-commerce in the region (responsible for 50% of all e-commerce in Latin America).

— The most purchased products by Latin Americans are, in order of demand: clothes, house utensils and electronic equipment.

— The most purchased services are those related to tourism (bus and airline tickets, car rental, booking of hotel rooms). For Brazilians, tickets for entertainment shows (concerts, shows, etc.) come in second, whereas Mexicans lead the purchases in online applications (software, games, music, video and in-app offers).

ONLINE CONTRACTS

Latin American countries still need to increase numbers of Internet users to exploit the full potential of e-Commerce[179].

Nevertheless, e-Commerce has been increasing in the region. International cross-border research conducted by PayPal shows that a significant proportion of online shoppers claim to make cross-border purchases in Latin America, and almost all cross-border shoppers also shop domestically. In Mexico the share of online shoppers that buy from national services is 38%, and in Brazil it is 50%[180].

When it comes to online shopping, 37% of consumers questioned in research conducted by IDC[181] indicated "safety" and "privacy" as the main issues preventing them from buying online.

This is followed by "limited payment methods" and "occurrence of fraud" as reasons to refrain from shopping online (59% of Colombian consumers are afraid of fraud while buying online). A behavioural reason also appears: 30% of consumers in Mexico and Brazil stated that they are not interested in online shopping at all.

National consumer laws are applied to online providers offering services within the jurisdictions of all analysed Latin American countries, regardless of their establishment within the countries' jurisdiction. This means that when an online retailer established in China or in a European country targets an Argentinian consumer, it is bound by the legislation on consumer protection in force in the targeted country.

Example 2 —
Regional harmonisation efforts for e-commerce in Latin America

Mercosur Resolution No. 21 (2004) [a/] on Consumer Information in Commercial transactions via Internet establishes that e-Commerce stores must make available to consumers clear, transparent, precise and easy-to-find information with regard to:

— the product and service characteristics;
— the commercial terms and conditions of the sale.

Mercosur Digital is a cooperation between Mercosur [b/] and the European Union aiming to consolidate the necessary structure for the digital economy in the region with benefits seen in Argentina, Uruguay, Brazil and Paraguay. The main objectives of this cooperation relate to e-Commerce and continued education. Five years after its establishment (2009-2014), the initiative managed to introduce digital signatures as legal instruments for the validation of digital contracts in all four countries.

Technological discrepancies were addressed in a "Plan of Digital Certification for Mercosur". Uruguay and Argentina adopted the "time seal" (or "time stamp"), a tool used as a token to guarantee the exact time of the signature of a digital document. Trusted time is important for digital signatures because it proves the date and time that documents have been signed, providing for stronger evidence that signatures were lawfully added at a point-in-time and that the data signed has not been altered since the signature was applied to it.

The countries also decided to introduce electronic invoices, also with the purpose of reducing tax evasion. Whereas in Paraguay Law 4610/2012 introduced the digital signature and implemented a certifying authority, in Brazil, authorities identified the need for harmonisation of the technology in the region. Uruguay and Argentina adopted Brazilian technology for the time seal of digital signatures.

The Trans Pacific Partnership Agreement (TPP)[c/] also has a set of rules for e-Commerce in its Chapter 14, recognising *"...the economic growth and opportunities provided by electronic commerce and the importance of frameworks that promote consumer confidence in electronic commerce and of avoiding unnecessary barriers to its use and development"*.

TPP brings further provisions related to taxation of electronic transmissions, non-discrimination of digital products (not applicable to broadcast rights) and recognises the importance of enhancing cooperation between their respective national consumer protection agencies or other relevant bodies on activities related to cross-border electronic commerce. The aim of such provisions is to enhance consumer welfare with respect to online commercial activities.

At global level, the UN agency on international trade, UNCITRAL, has been formulating harmonised rules on commercial transactions. These include: conventions, model laws and rules which are acceptable worldwide, legal and legislative guides, recommendations and information tools. UNCITRAL activities on e-commerce currently focus on e-signatures and trust services and dispute resolution platforms for cross border e-commerce[d/].

a/ Mercosur Res. 21/04 https://goo.gl/bqY5lZ Members of Mercosur are Argentina, Brazil, Paraguay, Uruguay and Venezuela
b/ Projeto Mercosul Digital: Novo Cenário para a Economia Digital no Mercosul, Oct. 2013. https://goo.gl/5rJ9qr
c/ Trans-Pacific Partnership, undersigned by Chile, Mexico and Peru (Colombia expressed an interest in joining, but is currently not part of the TPP). Chapter 14 on Electronic Commerce: https://goo.gl/rAH4jE
d/ UNCITRAL, working group activities III, IV and VI. https://www.uncitral.org/

TABLE 15

Overview of online contract laws and regulations in Latin America (Cullen International)

Laws and regulations addressing distance contracts	Specific law/regulations on the sale of digital goods and services	Do consumer safeguards of the country where the consumer is located apply to online providers located in another country?
The New Civil and Commercial Code of 2014. The code includes a definition of distance contracts, including those concluded by electronic means. The Civil Code (book 3, Title III) establishes some specific requirements for these contracts.	No Only general e-commerce regulations Resolution 104/2005 incorporating Mercosur Resolution No. 21 Consumer Information Law in Commercial transactions via Internet.	Yes Safeguards also apply to foreign companies offering goods/services to Argentinian consumers. The place of fulfilment of a consumer contract sets the applicable jurisdiction. Any clause establishing a different jurisdiction is prohibited by the Civil Code.
Consumer Code (Federal Law 8.078/90) Telecommunications Law (Federal Law 9.472/97) Decree 7.962/2013 expressly regulates electronic commerce	No Only general e-commerce regulations Consumer Code applies to distance contracts, including electronic and teleshopping contracts	Yes Safeguards also apply to foreign companies offering goods/services to Brazilian consumers and establish national jurisdiction. If a provider is not established in the country, liability can fall on any intermediaries operating locally on its behalf.
Law 19.496/97 (modified by Law 19955 2004) introduced e-commerce provisions.	No Only general e-commerce regulations Consumer Law applies to distance contracts, including electronic and teleshopping contracts	Yes Safeguards also apply to foreign companies offering goods/services to Chilean consumers (art. 50 Consumer Law)
Statute of Consumer Protection of 2014, has a chapter (V) on sales through non-traditional or distance methods, and a specific chapter for e-commerce (VI), both included by Regulatory Decree 1499/2014 (distance contract) and Decree 587/2016 (electronic commerce)	No Only general e-commerce regulations	Yes Safeguards also apply to foreign companies offering goods/services to Colombian consumers (art. 2 of the Statute of Consumer Protection)
The Federal Commerce Code regulates in general all types of contracts Consumer protection provisions for all transactions, including distance transactions, are included in the Federal Consumer Protection Law	No Only general e-commerce regulations	Yes The Consumer Law states that it applies in Mexico, without prejudice to the international treaties undersigned by the country (art. 1). A broad definition of provider (art. 2) covers foreign companies offering goods/services in the Mexican market.
Not specifically on distance contracts, but the Civil Code allows for the agreement and/or expression of will (Law 27291/2000) through electronic or other indirect means. It considers contracts between absent parties, including through electronic means.	No e-Commerce regulations apply to digital signatures (not to the sale of goods and services through the Internet).	Yes The Consumer Law (29571/2010) states that it applies to consumer relations conducted in the country or whose effects are produced within the country (art. 3,II).

Latin America does not count as a regional integrated market. Some level of harmonisation of consumer laws related to Internet transactions is found under Mercosur's rules, as seen in the box below.

The absence of a local establishment of international retailers targeting consumers in Latin America can however make the enforcement of consumer laws by national authorities difficult.

Nevertheless, in all countries analysed, administrative and judicial authorities have powers to authorise the inclusion of third parties as potentially liable for infringements. The principle of solidarity between players in the supply chain applies to online services and may hold banks, internet service providers, domain name registries, registrars, and hosting service providers, among others, (co)responsible for infringements.

This means that persons or companies having a presence in the country and acting as an intermediary for an international person or entity may not only be obliged to provide information for the identification of websites owners, but may also end up being considered liable in their own right.

A foreign company targeting the sales of online plane tickets to Brazilian consumers, for example, would use a Brazilian service provider to register its local domain name (.br). In the case of a consumer law infringement, if the foreign entity cannot be prosecuted during the process, the law would give the consumer the possibility of including the domain name service provider in the complaint or lawsuit, who could be held responsible on behalf of the website owner, as primary service provider[182].

At national level, Argentina, Brazil, Chile, Colombia, Mexico and Peru have already implemented e-commerce laws. In all countries the national rules also apply to enterprises established outside the national borders but targeting national consumers, as indicated in the Table below.

DIGITAL SIGNATURE IN LATIN AMERICA

Digital signatures are regulated in all large Latin American countries, with equivalence to physical signatures and validity beyond national borders recognised by laws.

The validity of digital signatures varies according to the international agreements that parties are affiliated to:

— Argentina and Brazil apply Mercosur rules with regard to digital signatures, but not to e-commerce in general, due to the lack of agreed Mercosur rules on e-commerce;

— Bolivia, Colombia and Peru apply Andean Community rules;

— Chile, Mexico and Peru apply Transpacific Partnership (TPP) rules.

Mercosur countries[183] have agreed on a common framework for electronic signatures regulation that resulted in the adoption of the same technological model for the infrastructure of public keys (security) and the same legal structure for the recognition of electronic signatures (validity). This has enhanced the transactions between the countries of the bloc and reinforced their credibility for countries around the world, especially in the EU[184].

With Decision 571 of the **Andean Community**[185], for the import of goods from Bolivia, Colombia, Ecuador and Peru, the use of digital signatures shall be promoted for the value declaration made to customs authorities. Decision 775 also enables the establishment of proof of origin for goods

imported by Members through a digital certificate, with a digital or electronic signature, insofar as an accredited authority has issued them[186].

Article 14.6 of the **Transpacific Partnership (TPP)**[187] is dedicated to electronic authentication and electronic signatures. It establishes that a party shall not deny legal validity of a signature solely on the basis that the signature is in electronic form. Furthermore, no party shall adopt or maintain measures that would prohibit or prevent parties to an electronic transaction from mutually determining the appropriate authentication methods for that transaction.

An authority accredited in accordance with domestic law may establish the methods of authentication and assure that they meet certain performance standards. According to TPP, Chile, Mexico and Peru shall also encourage the use of interoperable electronic authentication[188].

The three systems observed in the region are independent from each other, and membership of countries do not overlap[189]. This means, briefly, that:

— Mercosur has a broader integration, with one single technology, one guideline for harmonised regulation, and recognition of security and validity within the block

— The Andean Community has more general rules, focused on customs procedures, directed to the recognition of validity of digital and electronic signatures

— The TPP outlines common legal obligations to be implemented domestically and the recognition of an accredited authority.

Although some countries are associate members or observers of more than one system, no cooperation between the three systems for the harmonisation of digital and electronic signatures and mutual recognition is in place.

E-PAYMENTS IN LATIN AMERICA

The increased penetration of mobile services and internet access have increased the demand for instruments and tools for electronic transaction payments. These high levels of mobile penetration contrast with the low rate of credit/debit card penetration in the region, making e-payments, and particularly m-payments, a growing means of payment for both electronic and regular transactions.

M-payments are growing in the region. According to GSMA studies[190], by December 2014, 65% of Latin American markets had some sort of m-Payments application or service available to citizens. At end of 2014 there were 14.9m registered m-Payments accounts, of which 6.2m were active.

M-payments are used in Latin America for different purposes, with airtime top-up and Person to Person (P2P) transfers being the most important ones.

According to the GSMA studies, 50% of the usage volume in Latin America is for airtime top-up and 23% for P2P. Other relevant services used were bulk disbursements, and bill payments. Only 2% were for merchant payments. The world figures reflect 62.3% for air time top up, 25.1% for P2P, only 2.3% for bulk disbursements and 1.3% for merchant payments. The higher number for bulk disbursements in Latin America compared to the global figures might reflect the fact that mobile incoming payments are becoming a regularly used tool for payment and money transfer.

Regarding regulation, some countries like Paraguay, Peru and Colombia have designed specific regulations for e-payments systems, even creating special financial entities that offer their services through electronic means.

Example 3 —
m-Payments in Peru

Peru is one of the few countries in the Region to have developed a specific regulatory framework for the introduction of e-payment services.

As a means of increasing banking services penetration, the National Bank Association of Peru has created BIM (Electronic Wallet). This service is an m-payment and transaction application, backed by all the banks and e-payment entities in Peru. It allows all interested mobile phone users to have access to m-payments without owning a bank account or a credit card. Once the service is activated, end users can make payments, receive deposits, or withdraw from ATMs[a/].

Peru has created a well developed e-payment regulatory environment where licensed e-payment entities have specific obligations towards consumers and businesses, as well as obligations to guarantee transactions in a secure and private ecosystem.

Electronic Money Law 29985 of 2012[b/]:

— Provides a definition of e-money

— Establishes that the activities of e-money providers are supervised and regulated by the Superintendence of Banks, Insurance and Pension Funds as defined in the General Financial System Law (Law 26701/96). The Superintendence must also ensure interoperability of e-money services (i.e. possibility for a client to make transactions with any party, regardless of the provider of e-financial services)

— E-money firms need to comply with money laundering and terrorism prevention provisions, and must also comply with the data privacy and data protection provisions specified in the Personal Data Protection Law (Law 29733/11)

— Defines obligations of e-money providers towards consumers

— Established a VAT exemption on e-money providers for a period of 3 years from entry into force of the Law

Providers of telecommunications services must ensure equal treatment of the e-money providers. Osiptel to ensure equal treatment and resolution of disputes between providers of e-money services and telecommunications providers.

a/ For more information: http://mibim.pe/
b/ Law regulating the basic characteristics of electronic money, as a means of financial inclusion, 2012 https://goo.gl/Ca4vAw

These entities receive a licence or permit from the financial authorities superseding the electronic transactions system. These institutions are different from regular banking institutions and have special requirements and responsibilities towards consumers and businesses.

Implementation of e-Payment (including M-payment) models in Latin America differ: from strict regulatory schemes that require licensed intermediaries to manage e-transactions and e-money, to fairly open models which are usually backed by mobile payments firms or e-payment branches from banks or credit card companies.

As with other electronic transactions, data protection and other quality and security obligations are relevant to the participating parties. Specific to financial transactions, data encryption and guaranteed funds are also relevant to e-payment regulation. All surveyed countries require the same fund guarantee for e-payment transactions as for any regular bank transaction.

Special concerns arise with regards to the implications of e-Payments and e-Money for money laundering and other illegal transactions. For example, in the case of Peru, e-payments entities must specifically comply with anti-laundering and counter-terrorism regulations.

In Chile, where e-Payments have had a similar development as in the rest of the region, they are not covered by any specific regulation and are considered a complement or value added service offered over licensed mobile networks. Commercial terms and conditions apply for these services in contractual relations between service provider and users.

E-Payment options continue to develop in Latin America. Although there is domestic promotion for their growth and in most cases an appropriate regulatory framework, there are no significant regional initiatives or efforts for a coordinated development of these services in the region.

TAXATION IN LATIN AMERICA

Fiscal policies vary considerably across Latin America. Some countries promote the offer, adoption and usage of information and communication technologies (ICT) by reducing the tax burden, while others apply specific taxes, mainly on telecommunications services, increasing the cost of access to ICT goods and services.

This situation makes it extremely complex to find a common path for more harmonised conditions for e-commerce at a regional level.

Among the largest countries, Brazil and Argentina have the highest tax burden for both consumers and companies. In these countries the ICT sector is charged with a combination of high VAT, high sector-specific levies, and high customs duties.

In these countries taxes applied to consumers can add more than 30% to the mobile bill. Many countries also apply some sector-specific tax. Argentina, Brazil, Colombia and Mexico apply an additional percentage on consumers' bills, in addition to VAT. These taxes end up affecting end-user prices.

Fiscal incentives in Colombia are used as a means for boosting access to ICTs by making connection devices more accessible to the general public with a zero-rate VAT and also by eliminating VAT to internet access for the poorest users in the country.

According to a report by the International Publishers Association – IPA, Latin American countries have largely harmonised their VAT/GST regimes, applying the same zero-rate to printed books and e-books. Argentina, Brazil, Colombia and Mexico are among these countries.

In Peru and Ecuador printed books are zero-rated for VAT, but e-books are subject to the standard VAT rate. Chile applies the regular 19% VAT to both printed books and e-books [191].

The corporate tax burden in Argentina, Brazil and Colombia is considerably high. The latest World Economic Forum's Global Competitiveness Report published on September 2015[192], confirms this situation. The ranking includes Argentina (1) Colombia (4) and Brazil (7) in the 19 countries with the highest tax rates in the world.

The total amount of taxes calculated by WEF is the sum of five different types of taxes and contributions payable after accounting for deductions and exemptions: profit or corporate income tax, social contributions and labour taxes paid by the employer, property taxes, turnover taxes, and other small taxes.

Regarding import and customs taxes, on the one hand Argentina charges a total of 36.48% customs duty plus VAT on imported connection devices, while Brazil imposes a whole range of taxes that could reach up to a 60% rate plus ICMS Tax[193]. High import duties serve the purpose of protecting local manufacturing or assembly operations, but introduce important distortions into the devices market.

On the other hand, digital products enter duty-free in Colombia, Mexico and Peru.

According to a recent ITU study[194], the current debate around taxation policy in the digital world economy entails multiple issues, from the appropriate level of taxation on capital equipment purchased by telecommunications operators to the taxation of internet sales; from the taxation burden imposed on consumers of digital goods and services, to territorial issues, regarding the appropriate fiscal regime applicable to providers of digital platforms such as Google and Facebook (taxation in the country of establishment or in the country where the service is offered and used in practice).

Taxation in the ICTs has been largely studied in several documents by regional organisations. CAF, ECLAC and Cet.la[195 196], GSMA[197], IIRSA[198] and Regulatel[199] have carried out studies analysing, mainly, the tax burden on operators and users, and

TABLE 16

Country	VAT printed books	VAT e-books	Standard VAT
Argentina	0%	0%	21%
Brazil	0%	17-19%	17-19%
Chile	19%	19%	19%
Colombia	0%	0%	16%
Costa Rica	0%	0%	13%
Ecuador	0%	14%	14%
Mexico	0%	0%	16%
Peru	0%	18%	18%
Paraguay	0%	0%	10%

its impact. Issues related to the digital economy like double taxation, tax asymmetry between physical and digital products, and VAT in place of consumption, are in some way covered in the above mentioned documents.

Double taxation problems are solved via bilateral double taxation agreements or commercial agreements, which normally cover corporate taxation but do not include specific rules for digital markets.

There is no regional initiative or agenda towards a harmonised approach on taxation for the global digital economy. In order to develop a regional digital market, industries and governments would have to discuss updates on taxation requirements on internet sales and services to make sure customers are charged, tax authorities are paid and tax burden is appropriate for the development of the digital ecosystem in Latin America.

8 —
AUDIOVISUAL CONTENT: GEO-BLOCKING AND EXCLUSIVITY RIGHTS IN LATIN AMERICA

In Latin America, distribution licences are negotiated on a country-basis by networks, studios and distributors and in a quite unregulated environment. This is due to the fact that national legislation of all Latin American countries evaluated by Cullen International leaves the matter of exclusivity of licences, transfer of ownership and/or of exploitation rights to the complete agreement of the parties.

At regional level, Mercosur does not have specific provisions for copyright protection and enforcement. Other regional agreements, such as that establishing the Andean Community[200], have proposed some general guidelines for the transference or the assignment of rights. Chapter 9 of Decision 351[201] states that:

— any transfer of the economic rights, and also authorizations or licenses for use, shall be understood to be limited to the forms of exploitation and other procedures expressly agreed upon in the relevant contract; and

— in no case may the legal or compulsory licenses provided for in the domestic legislation of Member Countries exceed the limits permitted by the Berne Convention for the Protection of Literary and Artistic Works or by the Universal Copyright Convention.

This means that the interpretation of contractual clauses has to be limited to the forms and conditions expressly agreed upon. Moreover, as opposed to patents, countries of Mercosur shall not include provisions related to compulsory licences in their copyright laws.

In all monitored countries, audiovisual producers enjoy exclusive rights conferred to them by authors (of screenplay writers and directors, for example) and performers (actors and singers, for example), by force of licence agreements. Copyright laws confer protection to authors and holders of neighbouring rights for a term that varies from 50 to 80 years, depending on the country.

In order to confer exclusivity on the rights transferred or licensed, the laws of all countries demand the existence of an express clause in the agreements. This means, if parties wish the licence to be exclusive it will have to be written in the agreement, and never assumed in its interpretation. This means that contracts without express exclusivity clauses maybe entered into by a licenser with more than one licensee for the same scope and territory. This is the only and main regulation directed to exclusivity found in the profiled countries, noting that it is common to all of them.

Although limitations and exceptions to copyright exist in the laws of all monitored countries, no provision is directed to limit the scope or the cases where a licence could not be exclusive, or when exclusivity would have to observe the balance between authors', rightsholders' and final users' interests. Brazil is the only exception, with its copyright law establishing that after a term of 10 years (from the signature of an audiovisual production agreement), exclusivity conferred by authors and performers is automatically deemed to be extinguished. The law establishes a mandatory termination of exclusivity and parties do not have room to agree otherwise[202].

It is worth noting that none of the analysed laws introduces the concept of a "final user" or a "consumer" of copyrighted content, thus still distant from concepts present in the digital environment. The fact that the laws in most of the countries come from offline times may be the reason for that. Chile is the only exception, with the reformed Intellectual Property Law introducing the concept of Internet service providers (ISPs), search engines and online infringers.

GEO-BLOCKING IN LATIN AMERICA

Networks and studios around the world negotiate content licences on an exclusive basis and by geographic area. This is valid for Latin American countries. However, the copyright laws in the majority of the countries analysed have not yet been fully adapted to the online environment, Chile being the only country to include express provisions in its intellectual property law.

Therefore, the enforcement of territorial and exclusive rights relies very much on contract law, on off-line copyright laws' provisions and mainly on technological geo-blocking measures. The lack of specific regulation of copyright enforcement in the online environment may be the reason why geo-blocking is not yet an issue for rightsholders, consumers or governments, as we will see in the next chapter.

Differently from the European scenario, consumer laws in Latin America can only be enforced within the limits of each national jurisdiction. This means that a Mexican user traveling to Argentina could not make a complaint against Netflix's practice of automatically rerouting the access of said user's account to the local content of Argentina. Discussions on a possible right to portability of subscribed content are not yet underway in the region.[203] Nevertheless, it is a fact that some users with more advanced technological skills would use a VPN to access the home country's or another country's content while using the services.

It comes as no surprise that geo-blocking is a vastly adopted practice in the region. Major online platforms offering video content in Latin America, such as Netflix, Google and Crackle (Sony) are using it to enforce exclusivity rights negotiated in the licences with content owners.

In Argentina, Brazil, Chile, Colombia, Mexico and Peru, the main platforms direct the user to local content, according to the IP address. Access to foreign stores is not possible, with the exception of Apple and PlayStation Stores, which allow access to their content according to the country of origin of the credit card and/or country where the user set up the account.

Measures taken by rightsholders to avoid the bypassing by users of geo-blocking are already in place. Netflix, for example, has announced measures to fight geo-blocking circumvention together with a clarification of its goal to expand its worldwide presence (currently in 190 countries). Until a worldwide distribution system is in place (i.e. one licence obtained from rightsholders for a global exploitation of an audiovisual work), the company will keep on enforcing the regional granted licences with the help of geo-blocking technologies.

INITIATIVES TOWARDS A MORE INTEGRATED AUDIOVISUAL MARKET

It is a fact that the Latin American region is comprised of countries sharing many cultural bonds, reinforced by the presence of a common language in most of them.

This fact, on one hand, could facilitate the distribution and circulation of digital content in the region (e-books, movies and games, for example). However, rules to foster smoother distribution of content in the online environment do not exist in the region, nor are they being debated. The overall picture of the internet in the region shows that it reproduces the same barriers found in the physical world.

In order to support the development of a regional online audiovisual market, industries and governments would have to tackle the following issues:

— The current existence of a very low percentage of locally produced content, with US productions dominating the markets.[204]

— The current dominance of the distribution market by international studios.

The circumstances led the Ministry of Culture in Brazil, for example, to announce investments of BRL 10m (US$2.8m) for the creation of a national VOD platform (the initiative known as the "Brazilian Netflix") to offer the streaming of local content with affordable or free subscription.[205]

While regional initiatives directed to gaining a broader share of the regional market are not an important topic in the agenda of national audiovisual sectors, in the public sector, some general proposals might start the debate for the development of a more integrated regional market. This is the case of Programa Ibermedia, an initiative promoted by *Conferencia de Autoridades Cinematográficas de Iberoamérica* (CACI[206]). The project was designed to be a platform with selected movies from Latin America, Spain and Portugal, but it also offers production incentives, educational programmes and includes the distribution of content from national public broadcasters in its VOD platform[207].

No concrete discussions on copyright enforcement have taken place in this forum. However, the goals of the project include:

— the development of a favourable environment for audiovisual productions and the creation of an Iberoamerican audiovisual market, through harmonisation of national laws;

— technical and financial assistance for independent coproductions in the region;

— education of audiovisual professionals and development of new technologies.

The establishment of an Iberoamerican audiovisual market is still at a very early stage. The absence of regional initiative addressing distribution topics, such as some level of regulation of agreed-on licences and in a second instance, consumers' rights and geo-blocking practices, may be because in the main Latin American countries such issues are not yet on national agendas.

FIGHTING ONLINE PIRACY IN LATIN AMERICA

Online piracy in Latin America is a great challenge to the rich and diverse cultural heritage of the region, and affects the capability to protect and foster the creation of a valuable online market.

However, the Latin American region is falling behind. Measures within the national borders are weak. Relevant authorities at regional level have not even evaluated the cross-border dimension of the problem.

According to the South America Television Piracy Landscape report by Netnames for anti-piracy association Alianza (January 2016),[208] in a single month:

— South American internet users made 66m individual visits to the top 20 BitTorrent portals and in total the peer-to-peer ecosystem attracted 46.1m users;

— 62.7m South American users visited at least one cyberlocker link site, totalling 51.6m visits to the top 20 direct download and top 20 streaming cyberlocker link sites;

— a subsequent 23.3m visitors accessed cyberlockers themselves, making a total of 182.8m visits to the top 20 direct download and top 20 streaming cyberlockers;

— An estimated 8.7m users across the ecosystem were responsible for 28.9m visits to the top 20 Live IPTV sites. Live IPTV rebroadcasting is a growing threat within the region, with premium content channels streamable for free, on a variety of different web venues, including heavy usage of blogging platforms such as BlogSpot as a means of sharing links to Live IPTV content. Crucially, it can be distinguished from other online streaming of unlicensed content by its focus on live content.

A press release from the same association[209] also announced that, each year, an average of 1.5m hours are consumed through the illegal streaming of IPTV, cyberlockers and peer-to-peer activities in the Latin American region.

LEGAL FRAMEWORK

Whereas all countries have the support of criminal laws to combat piracy, only Chile has reformed its copyright laws in order to fully adapt them to the digital environment.

The fight against online piracy in most countries in the region is undertaken by means of:

— enforcement of agreed-on clauses (copyright contracts)

— already existing offline laws (copyright and general civil and contract laws)

— specific provisions prohibiting the circumvention of technological protection measures (TPMs) such as digital rights management (DRM), existing in copyright laws conceived in an offline environment.

Argentina, Brazil, Colombia and Peru have no specific provisions for fighting online piracy in their copyright laws, with exceptions to some measures related to the prohibition of circumvention of TPMs and DRM systems. Discussion for a wide reform of the copyright law has been underway in Brazil since 2007.[210] The parliament's Commission for Cybercrimes in Brazil has discussed the harms caused by the placement of advertising on websites infringing copyright and how to combat this practice.

Losses for the audiovisual sector were estimated by the Commission at BRL 10bn (US$ 2.85bn).

As mentioned before, Chile is the only country having reformed its intellectual property law (2010)[211] to introduce specific provisions to fight online infringements and a set of liabilities and exceptions for ISPs (search engines included), (see box below).

At the regional level, Mercosur has discussed and approved protocols related to trademarks, industrial designs, geographical indications and designation of origins, with no decision covering copyright[212].

Mexico signed the ACTA (Anti-Counterfeiting Trade Agreement) in 2012, and is bound to introduce modifications in its copyright law aimed at tackling online piracy. Art 27 of the ACTA requires country authorities to force ISPs to disclose relevant information regarding online piracy[213]. However, no modifications have yet been performed on the related national laws.

Among the few initiatives and debates focusing on regional-level actions[214], we can mention the following:

Strategic plan for the Cultural Integration of Mercosur (PEICM). Adopted in June 2015, the plan establishes medium and long term strategies to support cultural integration, cooperation and exchange in the bloc. Among the guidelines we can find the promotion of the distribution of cultural goods and services and the creation of a digital environment with more coordination on the fight against online piracy.

Example 4 —
The Intellectual Property Law Reform in Chile

In 2010, Chile reformed its Intellectual Property Law[a/] to adapt it to the digital environment. The main changes were conducted in order to introduce new legal definitions applicable in the digital environment, establish new types of illegal behaviours and set liability and exceptions related to ISPs and search engines. Legislators also touched upon issues that had long been regulated in the EU, such as a reversed engineering, transitional digital copies and circumvention of DRM.

In brief, the reform, introduced by Law 20435 [b/] established that:

- **ISPs are not responsible for copyright infringing online content transmitted through their networks, provided they do not modify, edit, select recipients or start the transmission;**
- **ISPs are not mandated to monitor data or actively search for illegal activities of users;**
- **ISPs are not mandated to monitor files or hyperlinks stored in their information systems and allowing access to pirated content and cannot be liable for the storage, provided they:**
  - **do not have effective knowledge of such information**
  - **do not profit from the exploitation of such content**
  - **remove the content in an expedited form when ordered by a court.**

a/ Law 17336 as amended in 2010 https://www.leychile.cl/Navegar?idNorma=28933 Law 17336 as amended in 2010 https://www.leychile.cl/Navegar?idNorma=28933
b/ Law 20425/2010 http://www.leychile.cl/Navegar?idNorma=1012827

The Inter-American Cooperation Portal on Cyber-Crime[215] was created by the Organisation of American States (OAS) to facilitate cooperation and exchange of information on cybercrime among government experts of the Member States. The OAS supports inter-American legal cooperation. During the last meeting of Ministers of Justice and Attorneys Generals (REMJA)[216], conclusions and recommendations included a special chapter on Legal Cooperation in the region to combat crimes involving computers and other electronic equipment.

PRIVACY AND DATA PROTECTION IN LATIN AMERICA

Two international organisations have supported a harmonised approach on privacy and data protection in Latin America.

The Economic Commission for Latin America and the Caribbean (ECLAC) included in its digital agenda for Latin American and the Caribbean (eLAC2018) specific objectives related to a harmonised privacy and data protection framework[217]:

— Objective 8: Strengthen the digital economy and e-commerce at the national and regional levels, adapting consumer protection regulations to the digital environment and coordinating aspects related to taxes, logistics and transportation, electronic payment mechanisms and personal data protection, and providing legal certainty to promote investment in the ecosystem;

— Objective 19: Promote the security of and confidence in internet use, guaranteeing the right to privacy and the protection of personal data.

On the other hand, the Organization of American States (OAS) has been working on a set of legislative guidelines[218] to promote a harmonised approach on personal data protection in the Americas. These guidelines will be based on the 12 principles that drew on the frameworks from the European Union (EU), the Organisation for Economic Co-operation and Development (OECD)[219] and the Asia-Pacific Economic Cooperation (APEC)[220].

OAS PRINCIPLES FOR A REGIONAL DATA PROTECTION FRAMEWORK

The principles adopted in 2015 by the OAS are as follows[221]:

— Lawful and fair purposes: Personal data should be collected only for lawful purposes and by fair and lawful means.

— Clarity and consent: The purposes for which personal data is collected should be specified at the time the data is collected. As a general rule, personal data should only be collected with the consent of the individual concerned.

— Relevant and necessary: The data should be accurate, relevant and necessary to the stated purposes for which it is collected.

— Limited use and retention: Personal data should be kept and used only in a lawful manner not incompatible with the purpose(s) for which it was collected. It should not be kept for longer than necessary for that purpose or purposes and in accordance with relevant domestic law.

— Duty of confidentiality: Personal data should not be disclosed, made available or used for purposes other than those for which it was collected except with the knowledge or consent of the concerned individual or under the authority of law.

— Protection and security: Personal data should be protected by reasonable and appropriate security guards against unauthorized access, loss, destruction, use, modification and disclosure.

— Accuracy of data: Personal data should be kept accurate and up-to-date to the extent necessary for the purposes of use.

— Access and correction: Reasonable methods should be available to permit individuals whose personal data has been collected to seek access to that data and to request that the data controller amend, correct or delete that data. If such access or correction needs to be restricted, the specific grounds for any such restrictions should be specified in accordance with domestic law.

— Sensitive personal data: Some types of personal data, given its sensitivity in particular contexts, are especially likely to cause material harm to individuals if misused. Data controllers should adopt privacy and security measures that are commensurate with the sensitivity of the data and its capacity to harm individual data subjects.

— Accountability: Data controllers should adopt and implement appropriate procedures to demonstrate their accountability for compliance with these principles.

— Trans-border flow of data and accountability: Member States should cooperate with one another in developing mechanisms and procedures to ensure that data controllers operating in more than one jurisdiction can be effectively held accountable for their adherence to these principles.

— Disclosing exceptions: When national authorities make exceptions to these Principles for reasons relating to national sovereignty, internal or external security, the fight against criminality, regulatory compliance or other public order policies, they should make those exceptions known to the public.

MAIN USERS' RIGHTS

A summary of the main users' rights in all countries researched is listed below:

— User consent for collecting and processing personal data: In Mexico, a privacy notice is needed for collecting and processing data for marketing and profiling purposes. In Argentina user consent to data processing for marketing

and profiling is not necessary, but there is a consumer right for opt-out from having data used for direct marketing at any stage. In Chile and Peru using data combined from different sources or individuals (not directly related to any of them) does not require user consent. In Colombia, an opt-in consent from the data subject is required in order to send electronic marketing material. In Brazil, user consent to process personal data is formally needed, but a Personal Data Protection Bill[222] adopts the concept of 'legitimate interest of the collector' towards a more flexible approach, enabling companies to process personal data under the legitimate expectation of the individual. In this case, only the strictly necessary data must be stored, and anonymised whenever it is possible.

— Notification of data breaches: Users do not need to be notified in case of data breaches in all countries researched. Nevertheless, a Personal Data Protection Bill[223] was submitted by the Brazilian Executive branch to Congress proposing that companies should notify users affected by a data breach if it likely leads to personal damage.

— 'Right to be forgotten': the 'right to be forgotten' is widely accepted either by legislation or case law (for instance, in Brazil and Chile).

— Confidentiality of personal data: In all countries companies are obliged to ensure confidentiality of personal data collected and processed.

DATA RETENTION AND STORAGE

Data retention by telecommunications companies for law enforcement and criminal prosecution purposes is mandatory in Brazil, Chile, Colombia, Mexico and Peru. Data must be retained for different periods, varying from 6 months to 5 years.

Only Brazil has a specific provision for applications, requiring companies to store data for 6 months (but storing data for a longer period may be requested by a judicial ruling).

In Argentina, there is no data retention regulation, since the data retention law was declared unconstitutional by the Supreme Court of Justice in 2009.

No country researched requires data to be stored within its territory.

THE ROLE OF GOVERNMENTS

The role of governments in the data protection framework is still being developed in most countries, as summarised below:

— Data protection authorities: Argentina, Colombia, Peru and Mexico have specific data protection authorities that users can address in the case of non-compliance to data protection law. In Chile and Brazil, the judiciary is the only institution currently entitled to enforce data protection rules.

— Notifying data breaches to data protection authorities: Only Colombia currently requires companies to notify data breaches to authorities. In Brazil, a Personal Data Protection Bill[224] proposes that companies should notify a data protection authority (to be created) in case of data breaches.

— Sanctioning: In case of non-compliance, fines are generally imposed. In Mexico fines for non-compliance can reach up to US$1.5m. In Brazil, fines imposed by the judiciary can reach up to 10% of revenues in the country. Suspension of processing personal data in case of non-compliance is possible in Argentina, Brazil and Colombia. In Mexico fraudulent processing of personal data or causing data breaches is punished with imprisonment (up to 3 years when data controllers cause a security breach to a database under their control with the aim of obtaining an economic benefit and up to 5 years for fraudulently processing personal data).

CURRENT DEBATES AND RECENT DEVELOPMENTS

Some countries in Latin America have recently discussed new data protection laws or implemented mechanisms to enhance legal enforcement[225]:

— Mexico: a law for protecting data held by public entities is under discussion. The right to data portability and requiring a data protection officer will be covered by the new framework[226].

— Chile: the government intends to release a personal data protection bill in the near future.

— Colombia: the country recently created a National Registry of Databases[227] and is now discussing a bill proposing that all entities responsible for data processing should comply with the national data protection framework, regardless of where it is located.

Example 5 —
Data protection in the Brazilian 'Marco Civil'

Regarding personal data protection, the Brazilian internet bill of rights ('Marco Civil') establishes[a/]:

— a general right of internet users to privacy of internet communications, except in the case of a judicial order authorising interception;
— obligation of internet service providers not to give third party access to their registries of end users' personal data, connections and applications, unless the end users have given their explicit consent or in the cases foreseen in the law;
— internet access providers to store internet connection registries (information on internet connections, including time and duration, and IP address for sending and receiving data packets) for a period of 12 months;
— internet application providers to store internet application registries (information on the use of internet applications from a specific IP address) for a period of six months;
— internet access providers, providing connection, cannot keep registries on applications; and
— ISPs will not be liable for (civil law) damages due to third party content.

An implementing decree[b/] provides a few more indications on the implementation of the data protection and retention principles included in the Marco Civil:

— authorities accessing personal data must publish annual reports to inform citizens about the amounts of personal data requested and for what purpose they were used;
— telecommunications and over the top (OTT) companies must hold the minimum amount of personal data, which must be erased as soon as the purpose of their holding is fulfilled or if a legal deadline is reached;
— companies must hold the personal data in a structured format that facilitates access by the authorities; and
— security rules mandated on internet access and applications providers, who shall define the format and procedures on personal data retention, including on how the registries are set, maintained and accessed. The Brazilian Internet Steering Committee (CGI) shall provide guidance on technical and operational standards.

a/ b/ Available at: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm

CYBERSECURITY IN LATIN AMERICA

In 2004, the Member States of the Organization of American States (OAS) formally recognised that combating cyber crime and strengthening cyber resilience were imperative to economic and social development; democratic governance, and national and citizen security[228]. Member States also acknowledged that in order to effectively confront evolving cyber threats and vulnerabilities, users, operators, and regulators are in need of timely and accurate information.

International cooperation is also seen at different levels through different organisations and bodies, such as Unasur, Mercosur, ICANN, ITU, OAS or FIRST, the Forum of Incident Response and Security Teams. For example, the OAS, through its Inter-American Committee against Terrorism (CICTE) has been working with various security incident response teams (CSIRT) in the region.

However, to this day no homogeneous approach has been observed in Latin American towards cybersecurity: while countries like Argentina, Brazil, Colombia and Peru have defined specific cybersecurity strategies, other countries such as Mexico and Chile have so far not adopted any particular strategy, but have however introduced changes in the criminal codes —considering crimes if hacking protected computing systems and accessing or copying information in those systems— and launched other initiatives mainly regarding breach reporting. In addition to a general policy addressing cybersecurity, Argentina and Brazil have introduced changes into national laws to explicitly define and sanction 'electronic and informatics crimes'.

In Argentina for instance, a national programme on critical infrastructure and cybersecurity was established in July 2011[229]. Main objectives of the programme are:

— working with public and private sector to elaborate and update cybersecurity strategy with special attention to critical infrastructure

— managing reports on security breaches in the public sector and analysing course of action and centralising information on breaches, solutions and all cybersecurity information (ICIC-GICI group)

— coordinating response to possible attacks to critical infrastructure.

Laws 26388 of 2008 and 26904 of 2013 also modified the Argentinian penal code to include and typify cybercrime and cyber harassment[230].

Colombia was among the first Latin American countries to adopt a cybersecurity strategy, starting in 2009 with the recognition of information and data protection for systems using ICTs[231], following in 2011 with the approval of comprehensive Cybersecurity and cyber defence public policy guidelines[232]. Most recently, in April 2016, the National Planning Department (DNP) approved a new digital public security policy based on the digital security strategy adopted by the OECD in September 2015.

The new policy seeks to move from a strategy focused on national defence and security in the digital environment to a more comprehensive strategy focused on identifying, managing and preventing digital security risks in a digital environment. The policy set several strategic objectives, each with a specific action plan, including:

— improvement of institutional framework for digital security;

— development of a safe digital environment allowing socio-economic activities to develop in the digital world;

— empowerment of citizenship and government areas about risk management and cyber crimes;

— strengthening of national defence, improving the capacity to prevent, detect and manage cyber threats and to protect critical infrastructure; and

— creation of mechanism to allow cooperation between local, national and international interested parties.

There is only one initiative in common across all surveyed countries, the creation of computer incident response teams (CIRT or CERT) in charge of prevention against computer threats, computer incident response, information, awareness and training in computer security. The work of the teams is not limited to national borders but they also share information and collaborate with other teams in the region.

NEW REGULATORY DEBATES IN LATIN AMERICA

BIG DATA

Most Latin American countries are already debating big data issues, although no specific regulation is yet in place.

— Argentina and Colombia are ahead of other countries in collecting information and debating big data challenges and possible fields for regulation;

— The Ministry of Science and Technology in Argentina commissioned a study on big data in 2015. The results identified the main sectors to receive future investments and main directions for possible future regulation;

— In Colombia, a draft law was presented in 2015 and awaits the designation of a rapporteur in Congress;

— Argentina, Colombia, Mexico and Peru have approved specific legislation to protect personal data in the online environment, paving the way for future regulation of one of the main concerns related to Big Data, data ownership and protection of privacy;

— Chile has a law from 1999 on privacy, which is being reviewed and modernised. A constitutional reform to include data protection among fundamental rights has also been proposed in the past, though present efforts are directed towards the approval of a reform of the existing law.[233].

— Brazil is currently discussing a Personal Data Protection Bill[234], submitted to public consultation and presented to Congress in May 2016, to regulate and establish minimum standards for the use of personal data aimed at the protection of dignity and personality.

Example 6 —
Big Data in Argentina and Colombia

In Argentina, the Ministry of Science, Technology and Productive Innovation[a/] has published a milestone document aiming to foster national debate on the potential benefits of Big Data.

The document does not propose any specific regulation on issues such as data ownership, interoperability, usability and liabilities, and mainly focuses on technical issues, including by raising a number of concerns:

— Is the country in a position to take advantage of the benefits of a new society based on knowledge?
— Does the analysis of Big Data require a technological-communication platform?
— Is the country in a position to create such a platform?
— How does the limited infrastructure development impact the complex infrastructure needs for Big Data development?

Among the sectors and national institutions identified as already potentially capable of applying Big Data in their activities the Ministry found:

— Biotechnology. Argentina has invested in genome sequencing initiatives, medicine and bioinformatics. The Science Faculty of University of Buenos Aires (Facultad de Ciencias Exactas y Naturales de la UBA) has conducted studies that could be implemented in the agro-livestock sector (veterinary medicine and genome of species), for example;
— Climate. The capacity of the publicly owned ARSAT network could be combined with the public transport system, and used for the prevention of natural disasters and urbanisation plans.

In Colombia, a bill aiming to establish a legal regime for the activities of "operating" and "processing" massive data was presented to Congress in 2015[b/].

The bill sets definitions specifically regarding Big Data. Once approved, it will apply to information companies established in Colombia and to activities developed by these companies within the Colombian territory.

Under the proposed rules, information companies will have to register at the Ministry of Information Technology and Communication to operate in the Big Data market. Rights and liabilities of such operators are mainly related to data protection.

Compliance control and enforcement will be carried out by the Superintendence of Industry and Commerce, though its Personal Data Protection department.

a/ CIECTI 2015 - Big Data: Avances Recientes a Nivel Internacional y Perspectivas para el Desarrollo Local https://goo.gl/gMWrQu
b/ Proyecto para Reglamentar la Operación Masiva de Datos, N. 134/2015
https://goo.gl/dGUIxw

CLOUD SERVICES

According to analysts[235] investment in cloud services in Latin America is predicted to grow by 153% over the next three years, from the current US$1.1bn to US$2.8bn in 2018. By 2020, the region is expected to have 1.3bn connected devices, out of the 80bn devices expected to be connected worldwide. Brazil, Colombia and Mexico will be responsible for half of the expected revenues in the region.

In the six countries analysed by Cullen International for this study, cloud computing services are used by individual users, enterprises and the public sector. All countries accommodate datacentres of the major international players (such as Amazon Web Services, IBM, Google, Oracle, SAP and Microsoft). The hybrid model[236] is the dominant model for companies using cloud services in the region.

Brazil is the only country having established some level of regulation and special measures for cloud services. In particular, Brazil established a limitation to the tendering of cloud services by the public sector. A Decree regulated by an inter-ministerial decision[237] established that public administrations would contract cloud services from public or partly public companies only, through direct purchasing assignment (i.e. not requiring a tender procedure). Only equipment or services not offered by public

Example 7 —
Ascenty: regional presence of datacentre services in Latin America

Ascenty[a/], one of the national leading players in the Brazilian market, is in the process of expanding its presence to other Latin American countries.

Besides a privately-owned telecom infrastructure encompassing 3,600 km of fibre-optic networks as well as four data centres in Brazil, the company is building up a new data centre in Santiago de Chile. The infrastructure of the city, combined with the existing demand from Ascenty's clients were decisive for the company's choice. The company also plans the establishment of a data centre in Mexico by the end of 2016.

Whereas hardware, software and technical support are the basis for the provision of cloud services, security and availability are the main concerns of Ascenty. In order to gain competitiveness, it has obtained a number of specific certifications, complying with both US and European standards. It is also certified to offer a technological environment complying with international Payment Card Industry Data Security Standard (PCI-DSS) rules.

A high level of customisation of the services offered and the existence of contracts fixed in US dollars helped the company to position itself as a leader in the sector. A natural protection provided by these contracts against the heavy exchange variations suffered by the local currency resulted in an annual income of US$ 150m in 2015.

Ascenty concentrates its operations in the private sector only, having among its clients IT companies such as SAP, Tivit, Microsoft, IBM and Google.

a/ Source: https://ascenty.com/

companies could be acquired by private companies through a tendering process.

Regulation on the location of servers is also established for companies providing services to the Brazilian federal public sector. The Information Technology Secretary of the Ministry of Development issued guidelines in May 2016 on the implementation of a requirement that all companies providing cloud services to the federal public administration are obliged to keep their servers installed within the national borders, including backup servers[238].

IOT IN LATIN AMERICA

4G Americas in 2014 estimated 14.6m M2M connections in Latin America. According to the association, connections will reach 160 million over a decade.

In a 2015 study, GSMA estimated 16.1 million connections in 2014, which represents only 2% of the total mobile connections in the region. However, GSMA also forecast a significant growth in the coming years, expecting annual growth of around 25% until 2020, accounting for 7% of total connections by that year for IoT services[239].

IoT services and applications expansion in Latin America will require new regulatory and market conditions. Most regulatory issues related to IoT and M2M still need to be discussed in Latin America. The development of a proper regulatory environment that can foster IoT applications and their growth is fundamental. Some debate has begun in a few countries.

Colombia, Brazil and Chile are the countries with the clearest perspective for an IoT regulatory agenda, although no official position has been issued yet.

Brazil has already introduced specific measures aimed at fostering M2M development.

A law approved in 2012[240] reduced by 80% the FISTEL tax paid for each SIM card used for M2M devices. The tax reduction has been effective since 2014, when a decree defined M2M communications[241]. According to industry this tax reduction was not sufficient to stimulate IoT in Brazil. At end-2015, there were 3.9m connected devices in Brazil according to Anatel data[242].

The ministry of communications has created a task force group focused on machine to machine communications, inviting the industry, telcos, R&D institutes, academic entities, app developers, the Senate and the Chamber of Deputies to participate[243].

The National Social and Economic Development Bank (BNDES) also published a RFP to formulate a policy focused on IoT in Brazil[244]. The resulting plan should identify relevant bottlenecks and propose targets and policies to stimulate the development of IoT from 2017 to 2022.

The presidential decree establishing the Brasil Inteligente Programme[245] mentions M2M communications as a policy goal for the programme. The ministry of communications (now extinct) announced that it would consult on a National IoT Plan. No information is available on the next steps for the implementation of the plan.

Most countries in Latin America lack specific IoT regulations and definitions. As a service that implies the generation and usage of great amounts of data – some specific and private to users/owners of IoT-involved appliances and equipment – concerns are arising about the capacity of the current regulatory frameworks to deal with these implications.

All of the countries analysed for the study have a general legal framework to protect the usage and access to personal data on digital or electronic means. So far only Argentina has developed a set of guidelines[246] for software and App developers that can have direct application on IoT data protection issues. In particular, the guidelines recommend key steps to ensure privacy from the design phase while developing web applications, as well as the use of Privacy-Enhancing Technologies (PET), consisting of measures, instruments and applications protecting

Example 8 —
Colombia: getting ready for a flourishing IoT market

Colombia is a very interesting case of a regulatory environment taking important steps towards the construction of an IoT-ready market. Colombia has a general framework for data protection and security.

Colombia's data protection rules elaborate on certain principles that guarantee data protection, integrity and security. At the same time, the regulation grants end users access, change and deletion rights over their data.

The categorisation of abusive access to a computer system as a criminal infringement also contributes to a secure and certain data usage and protection environment.

Colombia's National Spectrum Agency (ANE) is also proposing to allocate up to 50 GHz of spectrum specifically for IoT applications[a/]. Spectrum allocation for IoT would be in different spectrum bands, and would be used on an unlicensed basis. The Agency's proposal is now being studied at the Ministry and the Regulator CRC.

a/ http://andicom.co/wp-content/uploads/2015/09/1.ANE-MS-2015-08-31-ANDICOM.compressed.pdf

privacy of information by the elimination or reduction of personal data.

Regarding security, the different legislations dealing with cybercrime and other electronic security breaches in the analysed countries, can be in general terms applicable to IoT applications and services.

In a few countries a debate has begun on how to plan and allocate resources – namely infrastructure and spectrum – for the future development of IoT.

In Colombia, the Spectrum Management Authority is studying the allocation of up to 50 GHz of spectrum for IoT applications. In Chile and Brazil, cooperation between manufacturers and operators has been promoted in order to allocate financial and infrastructure resources for IoT development.

COLLABORATIVE ECONOMY: UBER IN LATIN AMERICA

The debate on the collaborative economy is very recent in Latin America, and it was triggered by the entry of Uber into the major cities of the region.

Controversy has mainly been around Uber-like and Airbnb-like services, and national and local government studies and decisions have been focused on trying to adapt regulation to these new forms of business.

In Argentina courts have banned Uber's services. In April, the day after Uber launched the service in Buenos Aires City, a court ordered the suspension of the operation in the capital city. The ruling came after an appeal by unions representing taxi drivers. On 5 May, the court decision was ratified by the Chamber of Appeals of Buenos Aires that confirmed the preventive closure of its digital platforms and apps. The City Attorney of Buenos Aires ordered regulator Enacom, as well as ISPs and mobile operators to block access

to Uber, following the Court order. However, and despite the ban, as of 16 May Uber is still functioning.

The first city in the region to regulate Uber has been Mexico City. Uber started operations in Mexico City in 2013. Mexico City taxi organisations claimed that the service was illegal, and that by not having to comply with regulations as the taxis do, Uber constitutes unfair competition.

In response, Mexico City's government held round-tables on how best to regulate Uber-like apps, and in July 2015 issued a regulation creating a new mode of public transportation through mobile apps. Regulations include the following:

— a monthly permit fee, per car, of MXN 1,599 (US$86) per car

— mandatory 1.5% per ride levy, in addition to VAT. The levy will contribute to a fund for public transit, roadways and pedestrian traffic, which will be used to improve taxi and app-based services

— vehicles value of at least MXN 200,000 (approx. US$10,700)

— drivers must register with the city's Transportation Secretariat, and will have to submit their vehicles to annual inspections

— a number of requirements for the vehicles like air conditioning, airbags and seat belts

— limitations on the company operations, such as not accepting cash or prepaid cards and not using taxi stands.

In Brazil Uber market entry was analysed by the competition authority CADE. According to the authority, Uber addressed a new, unexpressed demand from end users who did not make use of conventional taxi services[247].

In Rio de Janeiro, a court has enabled Uber to operate, despite a local government decision prohibiting the service.

In São Paulo, the City Hall issued a decree[248] regulating Uber-like services in May 2016. Companies are required to obtain a licence and pay a fee per km, which can vary according to city zone, time and type of car used (e.g. environmental friendly of not). Cars must be at maximum 5 years old, or 8 years if they have enhanced brakes (i.e. Anti-lock Braking System). Applications can mediate not-for-profit 'shared rides', which do not pay a fee per km.

In August 2016, the Brazilian Federal District, whose capital is Brasília, adopted the first law[249] regulating Uber-like services in Brazil. Requirements for companies are:

— Being a legal entity specialised in the provision of transport services (and no other activity)

— Being constituted in Brazil (and paying taxes locally)

— Being headquartered or represented by a branch in the Federal District

— Offering a car sticker with the logo by which the services are to be identified by passengers and the Social Mobility Office of the Federal District

— Accepting registration requests only from drivers presenting a valid certificate

— Paying the annual authorisation fee (amount to be defined)

— Presenting the prices of services in a transparent and comprehensible way to consumers.

A fee per km will be charged (amount to be defined).

Drivers are required to have no criminal records and obtain a certificate each year, paying an annual fee. Cars must be at maximum 5 years old, or 8 years old if they are environmentally friendly (using non-fossil based fuel). They also must have a minimum of 4 doors, air-conditioning and a maximum capacity of 7 passengers, be registered locally, purchase insurance against accidents and have a visible sticker with the logo of the application.

9 —
REGIONAL AND SUB-REGIONAL AUTHORITIES

One of the key enablers for the Digital Single Market Strategy in Europe is its institutional framework. In Latin America the situation is different, since there is a fragmented environment across the different countries and within groups of countries.

In Latin America we observe multiple regional initiatives in areas potentially affecting a digital market (connectivity, security, taxation, data protection, consumer protection, competition and regulatory frameworks, spectrum harmonisation and standardisation).

Most of these initiatives focus their efforts on research, capacity building or on the creation of forums of debate. Moreover, initiatives are sometimes run in parallel by these regional stakeholders, which however cannot impose or enforce decisions at regional or national level.

In this chapter we briefly analyse the digital economy activities of regional and sub-regional organisations in Latin America. Far from being an exhaustive assessment, the main objective is mapping what the main authorities are currently doing, and authorities aims at identifying the most

ORGANIZATION OF AMERICAN STATES (OAS)

According to the Charter of the Organization of American States[250], the OAS is an international organisation aimed at:

— achieving an order of peace and justice;

— promoting their solidarity;

— strengthening their collaboration

— defending their sovereignty, their territorial integrity, and their independence

The Organization uses a four-pronged approach to effectively implement its essential purposes, based on its main pillars: democracy, human rights, security, and development.

The OAS uses the following tools to pursue its goals:

— political dialogue (e.g. organising ministerial meetings on specific topics)

— cooperation (e.g. helping to implement technical reforms of electoral systems or providing training on trade negotiations and natural disaster mitigation)

— follow-up mechanisms (e.g. publishing reports to assess progress on a number of topics, e.g. the Mechanism for Follow-Up on the Implementation of the Inter-American Convention against Corruption)

— multilateral treaties (e.g. promoting legal cooperation on criminal matters and cyber-crime).

TABLE 17
OAS: digital ecosystem initiatives

Issue	Body / competence	Initiative adopted by the OAS
Data protection	The Department of International Law of the Secretariat for Legal Affairs, at the request of the General Assembly, prepared a study to provide a comparative look at the most prevalent systems for data protection, considering international instruments and national legislations on the topic. In 2015, the OAS adopted 12 principles on data protection that should be followed by Member States to achieve a harmonised approach. These principles drew on the frameworks from the European Union (EU), the Organisation for Economic Co-operation and Development (OECD) and the Asia-Pacific Economic Cooperation (APEC).	The Organization of American States (OAS) is now working on a set of legislative guidelines to promote a harmonised approach on personal data protection in the Americas. These guidelines will be based on the 12 principles previously adopted. Many countries within the region are now debating their data protection and privacy frameworks. According to the OAS, states should ideally follow these guidelines to have a harmonised approach.
e-Government	e-Government initiatives include a virtual campus (e-learning), MuNet (assisting municipalities using a toolkit to implement ICT tools in order to improve its administrative work, implemented in 22 cities so far) and RED GEALC (Network of e-Government Leaders of Latin America and the Caribbean). There is also a forum to promote best practices (Best Practices Forum of the Americas).	The Network of e-Government Leaders of Latin America and the Caribbean (RED GEALC) was created in 2003 as a joint initiative between the Executive Secretariat for Integral Development of the OAS and International Development Research Center (IDRC). RED GEALC promotes information exchange, including: — A reference environment for more than 60 senior officials responsible for implementing e-government in the countries of the region — Annual meetings to set priorities and learn experiences. — Awards for excellence in e-government, recognising the best solutions in transparency, citizen participation, efficiency, m-government, e-government citizen centred. — Establishment of a horizontal cooperation fund. — Research comprising Argentina, Brazil, Chile, Colombia, Ecuador, El Salvador, Mexico and Peru. — Technical workshops — Repository of information and documents updated daily and available online — A public software project — A database with nearly 300 experts of e-government. — training in e-government — A library of its own publications. — A monthly newsletter.
Cyber-crime	OAS promotes legal cooperation on criminal matters and cyber-crime	The OAS created the Inter-American Cooperation Portal on Cyber-Crime, which helps to streamline cooperation and information exchange on investigation and prosecution. It also promotes training to help states to develop legislation and procedural measures related to cyber-crime and electronic evidence (source).
Cybersecurity	OAS promotes legal cooperation on cybersecurity	The OAS promotes cooperation among CERTs (Computer Emergency Response Teams), e.g. hosting events to exchange information. It also publishes reports identifying trends in cybersecurity. Finally, it hosts the Observatory of Cybersecurity in Latin America and the Caribbean. It assesses the level of maturity of cybersecurity, considering: legal frameworks, technological issues, education and training, cybersecurity policies and cultural factors.
Electronic commerce and taxation	The Trade and Economic Development (TED) Section within the Department of Economic Development, provides support to OAS Member States to strengthen their institutional capacities to design and execute public policies and programs in the areas of micro, small and medium-sized enterprises and trade, including through training, horizontal cooperation and sharing of lessons learned.	The TED section implements training programs to strengthen the institutional capacity of governments. They also make available a Foreign Trade Information System (SICE), which provides access to information on trade policies in the Americas including: full texts of trade agreements in force, new and ongoing trade policy developments, national trade-related legislation, and links to international, regional and national sources. The information includes specific information on electronic commerce and agreements covering digital goods[a/].

a/ Information available at http://www.sice.oas.org/e-comm/e_com.asp

OAS AND CITEL

Today, the OAS brings together all 35 independent states of the Americas and constitutes the main political, juridical, and social governmental forum in the Hemisphere. In addition, it has granted permanent observer status to 69 states, as well as to the European Union (EU).

Relevant initiatives

The OAS has been working on a number of initiatives related to the digital ecosystem. A summary of these initiatives is shown below.

Within OAS, the Inter-American Telecommunication Commission (CITEL) seeks to "facilitate and promote the integral and sustainable development of interoperable, innovative and reliable telecommunications/ICTs in the Americas, under the principles of universality, equity and affordability".

CITEL structure for 2014-2018 includes:

— Assembly of CITEL

— Permanent Executive Committee (COM/CITEL)

— Permanent Consultative Committee I (PCC.I): Telecommunications/ICT

— Permanent Consultative Committee II (PCC.II): Radiocommunications

— Secretariat of CITEL

CITEL is used as a regional forum to provide inputs to international organisations such as the ITU.

The Permanent Consultative Committee I is the advisory body in the area of telecommunications/ICTs, in matters related to telecommunication/ICT policy, regulatory aspects, standardisation, cybersecurity, international public policy issues relating to the Internet, insofar as those issues involve telecommunications networks or ICT Infrastructure, universal service, economic and social development and the development of infrastructure and new technologies.

The Permanent Consultative Committee II is the advisory body in the area promoting the planning, coordination, harmonisation, and efficient use of the radio spectrum.

TABLE 18
CITEL action plan 2014-2018

Specific objectives related to the digital market in the Americas	Responsible parties
To identify and recommend best practices to reduce the digital divide among and within the Member States.	COM/CITEL, PCC.I, PCC.II
To produce and disseminate information and recommendations on best practices with regard to telecommunication/ICTs public policies and regulatory environment.	PCC.I, PCC.II
To promote the interoperability, harmonisation, regional mobility and connectivity of ICTs.	PCC.I, PCC.II
To foster discussions on public policy issues related to the Internet, particularly with impact on the increase of broadband penetration.	PCC.I
To enhance confidence and security in the use of telecommunications/ICTs, including cybersecurity, through increased collaboration between Member States and between CITEL and other international regional and sub-regional organisations and entities, including within the OAS.	PCC.I
To promote discussions on how to optimise the use of telecommunication/ICTs critical resources.	PCC.I, PCC.II
To promote capacity-building, training, technical cooperation, and technology transfer through CITEL's Regional Training Centers and organisations with which CITEL has cooperation agreements.	Secretariat of CITEL, COM/CITEL
To promote cooperation and coordination of activities, initiatives, projects, and programs with the International Telecommunication Union (ITU) and other international, regional, and sub-regional organisations and entities[a/].	Secretariat of CITEL, COM/CITEL, PCC.I, PCC.II
To expand and strengthen collaboration with the ITU Regional Office for the Americas in all matters related to telecommunication/ICTs, including on standardisation and radio communication issues.	Secretariat of CITEL, COM/CITEL, PCC.I, PCC.II
To elaborate and present documents and inter-American proposals at Study Groups and Conferences/Assemblies of the International Telecommunication Union (ITU).	COM/CITEL, PCC.I, PCC.II

a/ A complete list of cooperation agreements available at https://www.citel.oas.org/en/Pages/Cooperation-Agreements.aspx

The CITEL plan of action for 2014-2018[251] includes specific objectives in different areas, with a strong focus on infrastructure development, standardisation and harmonisation on telecommunications policies and the use of resources and synergies with ITU initiatives

ECLAC

"The United Nations Economic Commission for Latin America and the Caribbean", known as ECLAC, UNECLAC or in Spanish CEPAL, is a regional UN commission.

Headquarters: Santiago, Chile

Members: 45 States (20 in Latin America, 13 in the Caribbean and 12 from outside the region)

TABLE 19
eLAC 2018 strategy

Areas	Objectives
Access and Infrastructure	— Ensure universal access to digital content and production of content, with special emphasis on social inclusion — Promote regional coordination and efficient use of radio spectrum — Reinforce regional and sub-regional telecoms infrastructure, installation of new internet interconnection points (IXPs) and development of new content development networks (CDNs) — Stimulate investment in new generation broadband networks, including in rural areas — Support and cooperate in the adoption of digital terrestrial TV across the region
Digital economy, innovation and competitiveness	— Promote digital content, goods and services and stimulate the digital economy ecosystem, including though PPPs — Increase productivity by the use of ICTs, including by SMEs and microenterprises — Strengthen the digital economy and e-commerce at regional and sub-regional level, – adopting digital consumer protection rules – coordinating fiscal, logistics, payments, and data protection aspects — Stimulate policies on the strengthening of digital entrepreneurship at regional level
e-Government and citizenship	— Foster e-government by increased availability of such services — Create regional forums for regional exchanges and collaboration — Promote transparency and accessibility by citizens to government of public data by use of digital platforms
Sustainable development and inclusion	— Promote use of ICTs on the prevention and management of national emergency situations or disasters — Strengthen the use of ICTs in education — Increase quality and use of ICTs for the provision of health services — Promote telework, including its legal framework and exchange experiences on its monitoring and evaluation — Promote gender equality by use of ICTs — Ensure access to ICTs by vulnerable groups
Governance for information society	— Promote security and trust in the use of ICTs, ensuring privacy and personal data protection — Promote strategies and policies to fight cybercrime. Promote regional cooperation among incident response teams — Promote access to information and freedom of speech by use of digital media taking into account UN's ICCPR — Coordinate internet governance participation by Latin American and Caribbean countries — Foster the measurement of access and use of ICTs at national and regional level, strengthening institutional frameworks in the production of data and statistics

Associates: 13 members (which are various non-independent territories, associated island countries and a commonwealth in the Caribbean)

Role:

— to encourage economic cooperation in the region;

— research and knowledge creation and management (training activities included);

— issues contributing inputs and recommendations for the design and implementation of economic, social and environmental public policies, with an integrated approach to development in the countries of Latin America and the Caribbean.

Recommendations are nonbinding.

No dispute settlement mechanism for noncompliance is available.

Relevant initiatives

The ECLAC has been shaping, participating and contributing to the long-term process of regional technological cooperation.

This cooperation is part of the region's information society strategies stemming from the UN's World Summits on the Information Society and Millennium Declaration, and that have resulted in a series of Plans of Action for the Information Society in Latin America and the Caribbean (eLACs) in 2007, 2010, and 2015, adopted at different regional Ministerial Conferences[252].

Regional strategies have been evolving, from initial agendas mainly focused on bridging the digital divide, to more recent agendas that, in addition to connectivity and broadband as main targets also address the promotion of digital skills and capacities, e-government, innovation and digital entrepreneurship, as well as the application of technology in social domains (education and health).

New topics have gradually been addressed in recent debates, as summarised in the ECLAC study on "The new Internet Revolution"[253] and items included in digital agendas are now fostering digital innovation based on the use of public information, open government data, and the importance of Internet governance models based on multi-stakeholder involvement in policymaking.

At the last Ministerial Conference, held in Mexico City in 2015, countries renewed their cooperation agreements on digital issues with the adoption of eLAC 2018. The new strategy until 2018 includes 23 objectives in 5 main strategic areas, as summarised in the table below.

ITU-D

Name: The United Nations specialized agency for International Telecommunication Development Sector

Headquarters: Geneva, Switzerland

Members: 193 States (35 in the Americas). 700 members, including national regulators, companies and academia

Role:

— To foster international cooperation on telecommunication and ICT development issues

— To foster an enabling environment for ICT development and foster the development of telecommunication and ICT networks

— To enhance confidence and security in the use of telecommunication and ICTs

— To build human and institutional capacity, provide data and statistics, promote digital inclusion and provide concentrated assistance to countries in special need

— To enhance environmental protection, climate change adaptation and mitigation and disaster-management efforts through telecommunication and ICTs

Declarations are non-binding, however implementation of declarations and action plans are followed by periodic ITU-D reports to parties;

The latest ITU-D Action Plan was adopted for the period 2015-2018 at the latest World Telecommunications Development Conference in Dubai (2014). The Action plan includes 5 objectives:

TABLE 20
Relevant ITU-D initiatives in the Americas

Emergency communications	Assist Member States in all phases of emergency situations	Emergency telecoms plans for Central American and Caribbean countries Regional workshops
Spectrum management and DTT switchover	Assist Member States in the DTT switchover and in spectrum management	Events and forums in selected countries Technical assistance on cost models and prices Spectrum management plans in selected countries Assistance on trans-border agreements
Broadband development and adoption	Assist Member States in setting policies increasing broadband access and its use	Support to setting rural broadband policies in Central American countries Capacity building initiatives in the Caribbean Case study on Dominican Rep. Regional forum on cybersecurity, and IPV6 Support on fibre-optic cables developments in South America
Internet access and telecoms service cost reduction	Assist Member States in defining policies and mechanisms leading to wholesale and retail price reductions	Guidelines in roaming policies, laws ad regulations Forums, workshops and seminars on cybersecurity, IXPs, CIRTs
Trainings on global ICT policies incl. on cybersecurity	Increase digital skills in Member States and create enabling environment for ICTs	Sub-regional evaluation on the potential of mobile communications Workshops on internet governance, cybersecurity and data protection

— Foster international ICT cooperation

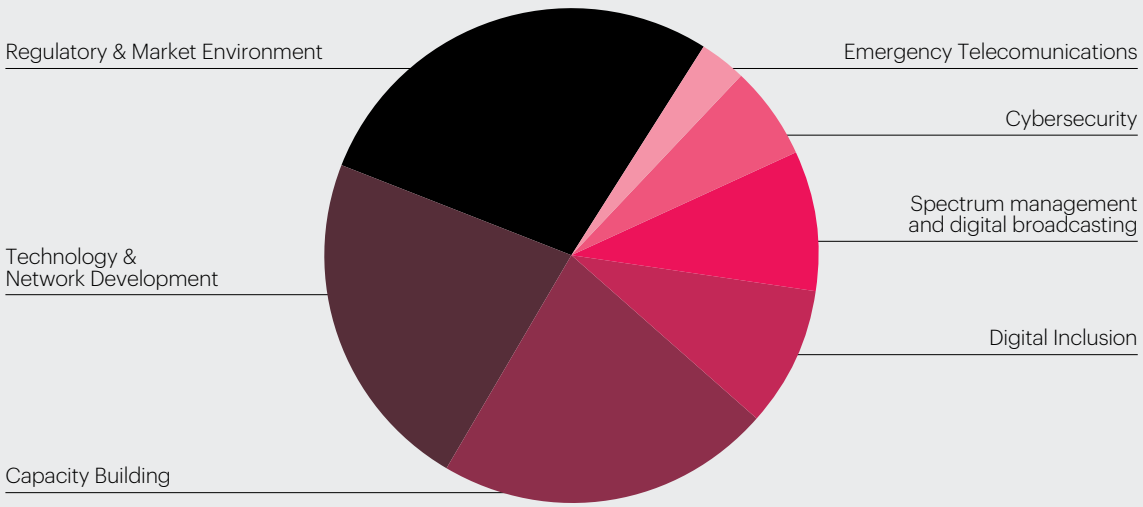
— Create an enabling ICT environment for network deployments and applications, including to bridge the normalisation gap

— Increase trust and security in the use of ICTs

— Human and institutional capacity building, especially in countries with special needs

— Use ICTs for environmental protection, climate change and to manage emergency situations.

FIGURE 16
Most of ITU-D projects in Latin America are focused on improving regulatory environment and network development (ITU-D)



REGULATEL

Regulatel is an association that brings together 23 telecommunications regulators, of which 20 from Latin America, and 3 from Europe, (Portugal, Spain, and Italy). Presence of Caribbean regulators is very limited and includes Puerto Rico, Dominican Republic and Cuba.

Regulatel objectives are:

— facilitating regulatory dialogue and information exchange between members

— promoting regulatory harmonisation in the region

— identifying and defending regional regulatory interests on international forums.

Regulatel agreements are not binding, and activities mainly consist of research and debate on different regulatory issues in the telecoms sector.

Regulatel current activities are currently organised in five working groups, each coordinated by a different regulator.

TABLE 21
Regulatel WG activities

Working groups	Main activities
Quality of service and user protection	Sharing experiences and best practices on the subject
Net neutrality and Internet issues	Monitors and reviews regulatory initiatives on net neutrality, and their impact
Competition in telecommunications markets	Sharing of information on experiences and strategies on the subject
Benchmarks	Creating an ICT indicators' data base for Regulatel members
Management and monitoring of radio spectrum	Collection and sharing of information on spectrum management across different countries

Regulatel also makes available to its members RedCLARA - Cooperación Latino Americana de Redes Avanzadas (Latin American Cooperation of Advanced Networks).

Developed with support from EU funds, RedCLARA, develops and operates the only Latin-American advanced Internet network connecting universities and research centres in 11 Latin American countries[254].

OTHER REGIONAL AND SUB-REGIONAL ORGANISATIONS

Activities related to the digital economy are developed by a number of other regional and sub-regional organisations. Among these, the ALADI, the CariCom, the Andine Community, the Mercosur, the Pacific Alliance, as well as the OECD, the UNCITRAL, or the WTO, just to mention a few.

In the table below we summarise the activities pertaining to DSM topics, by such entities.

TABLE 22
DSM-related activities carried out at regional or sub-regional level

Organisation	Subject	Coverage	Outcomes
ALADI	e-Commerce	Argentina, Bolivia, Brazil, Chile, Colombia, Cuba, Ecuador, Mexico, Panama, Peru, Uruguay, Venezuela	Recommendations and studies
ALADI	Taxation	As above	Customs agreements Recommendations and studies
FTAA-Alca	Taxation	Canada, Mexico, US	Customs agreement
Alizanza del Pacifico	Taxation	Chile, Colombia, Mexico, Peru	Customs agreements
Caricom	Cybersecurity	15 Caribbean nations and dependencies	Studies and discussion forums
Caricom	e-Commerce	As above	Regional e-Commerce platform
Caricom	ICT development	As above	Studies and non binding recommendations
Caricom	Taxation	As above	Customs agreements
CITEL	International Roaming	35 states in the Americas	Studies and discussion forums
CITEL	Spectrum harmonisation	As above	PCC-II: Radio communications: Technical recommendations, regional inputs for WRC
Comunidad Andina	Copyright	Bolivia, Colombia, Ecuador, Peru	Common regime
Comunidad Andina	Taxation	As above	Customs' agreements
ITU-R	Spectrum harmonisation	193 states (35 in the Americas)	Radio Assembly: Inputs for WRC, recommendations
ITU-R	Spectrum harmonisation	As above	Departments: Recommendations, reports
ITU-R	Spectrum harmonisation	As above	World Radio Conference (WRC): Radio regulations (technical)
ITU-T	International Roaming	As above	ITU-T Study Group 3: studies and recommendations ITU International Mobile Roaming (IMR) Resources Portal
ITU-T	Spectrum harmonisation	As above	Departments: Recommendations, reports
ITU-T	Standardisation	As above	Publications, resources, forums
Mercado Comun Centroamericano	Taxation	Guatemala, Nicaragua, El Salvador, Honduras, Costa Rica	Customs agreements
Mercosur	Taxation	Argentina, Brazil, Uruguay, Paraguay, Venezuela	Customs agreement Non binding recommendations
OAS	e-Commerce	35 states in the Americas	Foreign Commerce information system
OAS	Cybersecurity	As above	Inter-American Cooperation Portal on Cyber-Crime: Helps to streamline cooperation and information exchange on investigation and prosecution. Promotes training to help states to develop legislation and procedural measures related to cyber-crime and electronic evidence

Continued on next page →

Organisation	Subject	Coverage	Outcomes
OAS	Cybersecurity	As above	Promotes cooperation among CERTs (Computer Emergency Response Teams). Publishes reports identifying trends on cybersecurity. Hosts the Observatory of Cybersecurity in Latin America and the Caribbean
OAS	Data protection	As above	Department of International Law of the Secretariat for Legal Affairs: Adopted 12 principles on data protection that should be followed by Member States to achieve a harmonised approach and is drafting legislative guidelines to promote a harmonised approach on personal data protection in the Americas
OAS	e-Government	As above	The Network of e-Government Leaders of Latin America and the Caribbean (RED GEALC): Promotes information exchange
OECD	Security	34 states, of which only Chile and Mexico from Latin America	Studies, statistics
OECD	Privacy	As above	Guidelines Recommendations on enforcement
OECD	e-Commerce	As above	Consumer protection guidelines e-Commerce recommendation. Studies and guides
OECD	Digital identity and e-Authentication	As above	Studies, recommendations
Regulatel	International Roaming	23 regulators of which 20 from Latin America	Exchange of information
Regulatel	Net neutrality	As above	Working group on net neutrality: Information and benchmarks.
Regulatel	Spectrum harmonisation	As above	Working group on spectrum management and monitoring: Information and benchmark on best practices related to spectrum management and monitoring, including the use of new spectrum frequencies.
UNASUR (Cosiplan/ IIRSA)	Infrastructure integration	Argentina, Bolivia, Brazil, Chile, Colombia, Ecuador, Guyana, Paraguay, Peru, Suriname, Uruguay, Venezuela	Broad initiatives aiming at fostering infrastructure investment and increased, integrated network facilities in South America
UNCITRAL	e-Commerce, e-Identity	Argentina, Bolivia, Brazil, Canada, Chile, Colombia, El Salvador, Honduras, Mexico, Paraguay, US, Venezuela	Activities within WG 4 on electronic commerce. Studies, model laws
UNCITRAL	Online dispute resolution	As above	Studies, model laws within WG 3 on dispute resolution mechanisms for online cross-border transactions.
UNCITRAL	Secure transactions	As above	Studies, model laws within WG 6 on secured transactions.
WTO	e-Commerce	192 members, of which 30 from the Americas	Work Programme on Electronic Commerce. Declaration on global e-commerce, seminars, study groups on the application of current trade agreements to electronic commerce

10 — CONCLUDING REMARKS: MAIN OBSTACLES HAMPERING THE CREATION OF A DSM IN LATIN AMERICA

The EU and Latin America each have a population of approximately 500 million. Building a 'digital single market' of 500 million consumers is an attractive perspective in economic and social terms, in the EU as well as in Latin America.

In this study we have addressed a number of elements that, in the European Commission's strategy, are indicated as 'key' to reaching the DSM goals in Europe.

While reviewing such topics, we have also analysed whether and how Latin American countries are addressing the same topics, and whether any concrete harmonisation initiative is already observed at regional level for each of those topics.

There is a conceptual challenge in comparing the EU's existing single market approaches with a potential, prospective Latin American single market.

Latin America – as opposed to the EU – is a group of individual nations within a very large, and diverse geographic region. These countries often share similar cultural identities and languages, but are still lagging behind in reaping the full benefits stemming from a more intense regional trade, or in trying to establish economic and social development policies in a more coordinated way.

The idea of building a DSM for Latin America could be considered as particularly challenging and ambitious, as no single telecommunications market or single trade area covering the entire region has so far been created.

Far from being an exhaustive study on each of the components and challenges of the EU DSM strategy, in this report, in addition to an overview to the EU approach, we have also discussed for Latin America:

— the existing conditions for digital networks and services; and

— how consumers and businesses currently benefit from online goods and services.

Unsurprisingly, the study recognises that while the EU has already identified what are its own remaining 'gaps', as well as a precise roadmap for the achievement of a more integrated and consistent regional approach for a DSM, in Latin America this debate has just started.

There is no clear consensus among Latin American nations today on the desirable level of regional integration. Therefore, building a DSM for Latin America would also require a 'single' regional vision on the future of its societies and economies.

Individual Latin American countries have been addressing policy or regulatory challenges related to increasing internet connectivity or to stimulating their own digital economies mostly independently from one another.

A few regional and sub-regional initiatives are already observed across Latin America, as summarised in Table 1 and IP Interconnection in this report. Apart from a few customs agreements on taxation by sub-regional entities, most of the initiatives today are aimed at collecting, analysing and sharing information, drafting guidelines, or at debating current challenges and exchanging country experiences at regional level.

Fragmentation at regional level is often combined with overlapping of efforts across the region.

Latin America lacks a common institutionally binding framework. However, a single DSM might still be a target for the region, provided there is a common vision, and capacity to put in place effective implementation efforts – including by means of adequate consensus methodologies and governance mechanisms.

The accomplishment of a DSM for Latin America would require a vision, and strong political commitment from the parties involved, to overcome different types of obstacles, within countries and between countries. This report does not hold the ambition of providing answers to such a fundamental and critical question.

Rather, we have attempted to draw a picture of the current situation in Latin America vis à vis individual topics currently at the core of the DSM debate, and identify possible "areas of improvement", which mainly relate to key obstacles observed today in several countries.

The potential improvements are grouped into two main areas: "connectivity" and "access to online goods and services".

In the table below we draw a summary of the possible objectives and actions for each improvement area. In the last column we report, as a reminder, the multilateral and international organisations currently implementing projects or activities in such areas. More coordination among existing (and future) initiatives might represent an objective in itself, as this would likely increase the effectiveness and efficiency of many such initiatives. However, once again it is not in the scope or objectives of this study to analyse either the effectiveness of the current initiatives or whether better alternatives might exist.

CONNECTIVITY

As highlighted in Part I, Chapter II.B.1, even in the EU and despite the presence of several industry groups operating in multiple countries, network infrastructure continues to be deployed, operated and owned at national level. Significant network inputs and resources, such as radio spectrum, numbers, licences or permits, are also administered by country authorities.

The EU has already addressed certain 'remaining gaps' for a telecoms single market, such as homogeneous regulatory treatment of International Roaming or Net Neutrality. Other significant objectives are however yet to be completed, and are part of the EU connectivity agenda, and the ongoing review of the regulatory framework of electronic communications.

Although presenting larger 'gaps' compared with Europe, improved harmonisation on the connectivity front might bring substantial benefits to the Latin America region.

TABLE 23
Improving connectivity within a Latin American DSM

Improvement areas	Key obstacles	Strategic objectives (to remove obstacles)	Possible actions	Main actors currently involved
International roaming	Prices remain high Double taxation is still an issue	Analyse main obstacles currently hampering the harmonisation of the international roaming services market in Latin America Assess impact of regulation, where implemented Define possible options — from industry self-regulation to regulatory intervention	Set up study group and common roadmap Direct involvement of industry and governments.	Regulatel National regulators Industry associations
Spectrum harmonisation	Insufficient harmonisation. No cooperation on new services and applications	Agree on future harmonised spectrum allocation and assignments in the region, including on new services (e.g. 5G)	Define roadmap towards increased spectrum harmonisation in Latin America	CITEL ITU Regulatel Industry associations
IP connectivity, IP interconnection	The region lacks sufficient IXPs Unclear regulatory approaches on IP interconnection Low interaction between commercial and non-commercial stakeholders Insufficient understanding of the role of new platforms	Increase connectivity and data network performance at regional level Foster the development of IXPs across the region Incentivise the creation of data centres in Latin America	Monitor and report on the development of IXPs in Latin America Analyse business models, actors and regulatory framework in place Analyse and discuss at regional level possible regulatory strategies for IP interconnection and to adapt regulatory models	Lack of coordination at regional level Insufficient dialogue between stakeholders, due to divergent interests
Regulatory frameworks	The national regulatory frameworks are often outdated and ineffective Lack of common, strategic vision at regional level	Adapt national framework to new challenges, in a coordinated and consistent way Ensure frameworks are effectively implemented	Carry out an objective, independent analysis on regulatory frameworks and functioning of NRAs across Latin America. Identify key performance indicators and toolkits on regulatory reviews	Lack of coordination at regional level Significant work could be carried out by Regulatel and ITU

ACCESS TO ONLINE GOODS AND SERVICES

As highlighted in Part I, Chapter IV, there are a number of obstacles still impeding EU citizens and businesses from fully enjoying the opportunities of a DSM.

In Latin America, similar challenges are observed. These concern for example the protection of copyright, the fight against online piracy, and the protection of citizens' privacy and security. Issues such as taxation are challenging the capacity to develop a regional DSM. Regulatory debates on the impact of emerging technologies and applications, such as cloud computing or M2M, are still at an early stage in all countries. When legislative or regulatory initiatives are present, these are conceived at national level. The end result is a considerably diverse and fragmented scenario.

In some cases, individual countries in Latin America have managed to put forward effective responses, even becoming best practice cases at the world level, as in the case of m-payments for example. But this is the exception rather than the rule. In the table below we discuss what could be done to improve this scenario.

TABLE 24
Aiming for better access to online goods and services within a Latin American DSM

Improvement areas	Key obstacles	Strategic objectives (to remove obstacles)	Possible actions	Main actors currently involved in these areas
Copyright and online piracy	Lack of common guidelines on copyright and fighting piracy Insufficient efforts on promotion of Latin American audiovisual content	Ensure adequate copyright protection and fighting of online piracy Foster development and circulation of Latin American audiovisual content	Guidelines and best practices on legislative, regulatory or industry measures to address current and future challenges. Funding mechanisms for the promotion and distribution of content	No relevant initiatives at regional level
e-Contracts, digital signatures, e-Payments	Lack of common guidelines and tools to increase trust and protection	Increase trust among consumers and businesses in buying / selling online	Guidelines on how to build trust and consumer protection at regional level Also study logistics aspects, including parcel delivery costs and performance within Latin America	UNCITRAL No other relevant initiatives
Privacy and data protection	Lack of common guidelines and tools to increase protection	Harmonise legal frameworks on privacy and data security at regional level, to increase certainty Define clear liabilities for all the actors involved	Study existing frameworks, exchange relevant information. Define possible harmonisation measures at regional level	OAS
Cybersecurity	Lack of coordinated efforts	Increase effectiveness of initiatives and increase scope at regional level	Define operational cooperation at regional level and relevant implementation authorities	No regional coordination

ENDNOTES

1. European Commission, Digital Single Market webpage http://ec.europa.eu/priorities/digital-single-market_en

2. COM(2015) 192 Final – A Digital Single Market for Europe. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN

3. The EU is composed of 28 European countries, namely: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, The Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and United Kingdom

4. Article 1 Treaty on European Union

5. Article 3 Treaty on European Union

6. Article 17 Treaty on European Union

7. Articles 14 and 16 Treaty on European Union

8. Articles 289 and 294 Treaty on the Functioning of the European Union

9. Article 2 Treaty on the Functioning of the European Union

10. Article 26 Treaty on the Functioning of the European Union

11. European Commission Communication 'A Digital Agenda for Europe', COM(2010) 245 final/2. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0245R(01)&from=EN

12. European Commission Communication 'A Digital Agenda for Europe', COM(2010) 245 final/2, Annex II

13. European Commission, Eurostat, ICT survey of Enterprises, 2014

14. European Commission, Eurostat, ICT survey of Enterprises, 2013

15. European Commission Communication 'A Digital Single Market Strategy for Europe', COM(2015) 192 final, page 4 - http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN

16. See EC Working Paper: Europe's Liberalised Telecommunications Market - A Guide to the Rules of the Game https://portal.etsi.org/erm/kta/harmstd/userguide-en.pdf

17. The regulatory framework at Community level establishes a set of minimum requirements which Member States are obliged to implement and enforce, with the detailed application of those principles and requirements being carried out at a Member State level. The use of Directives as the key legislative instrument in extending the internal market and competition rules to the telecoms sector means that implementation is left to each Member State to decide according to its own requirements and national legal system.

18. See the Commission website for an overview of infringement cases for incorrect implementation of the 2003 regulatory framework (https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/Infringement%20procedures%20opened%20for%20incorrect%20implementation.pdf) and late transposition of the 2009 EU regulatory framework for electronic communications (https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/Infringement%20procedures%20opened%20for%20non-communication%20of%20the%20revised%20framework.pdf)

19. The latest EC Implementation Report (n. 19) was published in June 2015. https://ec.europa.eu/digital-single-market/en/news/implementation-eu-regulatory-framework-electronic-communications-2015

20. EC Staff Working Document - A Digital Single Market Strategy for Europe - Analysis and Evidence Accompanying the document, page 34. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015SC0100&from=EN

21. E-communications and the Digital Single Market http://ec.europa.eu/information_society/newsroom/image/document/2016-22/sp438_eb84_2_ecomm_summary_en_15829.pdf

22. Broadband Market Development in the EU 2016 https://ec.europa.eu/digital-single-market/en/connectivity

23. Idem

24. The 800 MHz spectrum band is the first 'digital dividend' in ITU's region, covering most of Europe and Africa

25. Digital Agenda – Key Indicators https://digital-agenda-data.eu/datasets/digital_agenda_scoreboard_key_indicators/visualizations

26. Digital Economy and Society Index (DESI) https://ec.europa.eu/digital-single-market/en/desi

27. The Europe 2020 strategy/Digital Agenda set out the following targets for broadband deployment: by 2013, basic broadband (speed not defined) for all Europeans. By 2020, "fast" broadband with speeds of above 30 Mbps for all Europeans; 50% or more of European households subscribe to internet connections above 100 Mbps ("ultra-fast" broadband). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF

28. Lighter regulation in areas with infrastructure competition, to foster investment

29. Universal Service Directive 2002/22/EC. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:l24108h

30. First draft of the proposed Regulation. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0627:FIN:EN:PDF

31. Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015R2120. Parliament and Council expressed concerns about a possible higher involvement of the EU Commission over radio spectrum matters. Radio spectrum has always been within the competencies of individual Member States.

32. See Part I, Chapter II.B

33. The Body of European Regulators for Electronic Communications (BEREC) was established by Regulation (EC) No 1211/2009 of the European Parliament and of the Council of 25 November 2009, as part of the Telecom Reform package. BEREC contributes to the development and better functioning of the internal market for electronic communications networks and services. It does so by aiming to ensure a consistent application of the EU regulatory framework and by aiming to promote an effective internal market in the telecoms sector. BEREC assists the Commission and the national regulatory authorities (NRAs) in implementing the EU regulatory framework for electronic communications. It provides advice on request and on its own initiative to the European institutions and complements at European level the regulatory tasks performed at national level by the NRAs. The NRAs and the Commission must take utmost account of any opinion, recommendation, guidelines, advice or regulatory best practice adopted by BEREC. http://berec.europa.eu/

34. The Radio Spectrum Policy Group (RSPG) is a high-level advisory group that assists the European Commission in the development of radio spectrum policy. As part of its advisory function, the RSPG consults extensively and in a forward-looking manner on a variety of technological, market and regulatory developments relating to the use of radio spectrum in the context of relevant EU policies. Such consultations are conducted with the objective of involving all relevant stakeholders, radio spectrum users, both commercial and non-commercial, as well as any other interested party. Most of the deliverables of the RSPG are subject to formal public consultations. http://rspg-spectrum.eu/about-rspg/

35. Joint BEREC/RSPG statement of Feb. 3, 2016. http://berec.europa.eu/eng/document_register/subject_matter/berec/press_releases/5663-joint-berecrspg-news-release-on-spectrum-and-the-framework-review

36. EU Commission – 2013. Proposal for a Regulation laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC and 2002/22/EC and Regulations (EC) No 1211/2009 and (EU) No 531/2012. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0627:FIN:EN:PDF

37. Regulation (EU) 2015/2120 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015R2120

38. COM(2013) 627 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0627:FIN:EN:PDF

39. Nkom note on Net neutrality and charging models http://eng.nkom.no/topical-issues/news/net-neutrality-and-charging-model

40. NRA must report annually to the Commission and BEREC on their findings. BEREC issues guidelines to the NRAs on the implementation of this activity.

41. The maximum surcharges are: for outgoing calls: 5 €cents per minute for text messages: 2 €cents for data: 5 €cents per megabyte. For incoming calls, the maximum surcharge will be the weighted average of maximum mobile termination rates across the EU, to be set out by the Commission via an implementing act by 31 December 2015.

42. EC Impact assessment of the EU Roaming Regulation, June 15, 2016 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0201&from=EN

43. Directive 2002/20/EC http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0020

44. Hernán Galperín, Localizing Internet infrastructure: Cooperative peering in Latin America (2016) http://annenberg.usc.edu/sites/default/files/2016/01/25/published%20article_0.pdf

45. Exmansion de la Infraestructura Regional para la Interconexion de Trafico Internet en America Latina, CAF, 2014 http://publicaciones.caf.com/media/41097/expansion_infraestructura_internet_america_latina.pdf

46. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF

47. Under the Radio Spectrum Policy Programme established by Decision 243/2012/EU of 14 March 2012 in support of the Digital Agenda, the Commission decided to implement an EU Radio Spectrum Inventory.

48. Commission Staff Working Document: A Digital Single Market Strategy for Europe http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015SC0100

49. ITU-R Report M.2290-0 (12/2013) on Future spectrum requirements estimate for terrestrial IMT, available at http://www.itu.int/pub/R-REP-M.2290-2014

50. When the European Commission adopts implementing measures under EU law, it may be subject to the control of committees of Member State representatives, established by the relevant legislation. There are around 250 such committees covering a wide range of different subjects. Each committee is made up of experts representing the Member States and chaired by a non-voting representative of the Commission.

51. European Commission draft Decision on the use of the 470-790 MHz band of Feb. 3, 2016. http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1454410061980&uri=COM%3A2016%3A43%3AFIN

52. Harmonised technical conditions of use in the 790-862 MHz frequency band for terrestrial systems capable of providing electronic communications services in the European Union. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:117:0095:0101:EN:PDF

53. Commission Decision 2009/766/EC of October 16, 2009 on the harmonisation of the 900 and 1800 MHz frequency bands for terrestrial systems capable of providing pan-European electronic communications services in the Community. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:274:0032:0035:EN:PDF

54. /251/EU: Commission Implementing Decision of 18 April 2011 amending Decision 2009/766/EC on the harmonisation of the 900 MHz and 1800 MHz frequency bands for terrestrial systems capable of providing pan-European electronic communications services in the Community. http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32011D0251

55. (EU) 2015/750 of 8 May 2015 on the harmonisation of the 1452-1492 MHz frequency band for terrestrial systems capable of providing electronic communications services in the Union. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015D0750&qid=1433954639520&from=FR

56. Commission Implementing Decision of 11 December 2013 amending Decision 2006/771/EC on harmonisation of the radio spectrum for use by short-range devices and repealing Decision 2005/928/EC, available at http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1431504940344&uri=CELEX:32013D0752

57. Commission Decision of 23 November 2006 on harmonisation of the radio spectrum for radio frequency identification (RFID) devices operating in the ultra high frequency (UHF) band, available at http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32006D0804

58. REGULATION (EU) No 1025/2012 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 October 2012, available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32012R1025

59. The European Multi Stakeholder Platform (MSP) on ICT standardisation was set up at the end of 2011. Based on a European Commission Decision to advise on matters related to the implementation of ICT standardisation policies, it deals with: potential future ICT standardisation needs in support of European legislation, policies and public procurement; technical specifications for public procurements, developed by global ICT standards-developing organisations; cooperation between ICT standards-setting organisations; the Rolling Plan, which provides a multi-annual overview of the needs for preliminary or complementary ICT standardisation activities in support of the EU policy activities. The MSP is composed of representatives of national authorities from EU Member States & EFTA countries, of the European and international ICT standardisation bodies, and of stakeholder organisations that represent industry, small and medium-sized enterprises and consumers.

60. European Commission, Flash Eurobarometer 397, 'Consumer attitudes towards cross-border trade and consumer protection', 2014 , page 5 - http://ec.europa.eu/public_opinion/flash/fl_358_en.pdf

61. European Commission, Flash Eurobarometer 413, 'Companies engaged in online activities report', 2015, page 12

62. http://ec.europa.eu/priorities/sites/beta-political/files/dsm-factsheet_en.pdf

63. Article 56 of the Treaty on the Functioning of the European Union and article 16 of Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market – Services Directive - http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1463049714449&uri=CELEX:32006L0123

64. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market – e-Commerce Directive - http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1463049771328&uri=CELEX:32000L0031

65. Article 4 e-Commerce Directive

66. Article 6 Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) - http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1463049839125&uri=CELEX:32008R0593

67. European Commission, Flash Eurobarometer 413, 'Companies engaged in online activities', 2015, page 21 - http://ec.europa.eu/public_opinion/flash/fl_413_en.pdf

68. Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council - http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1463050720619&uri=CELEX:32011L0083

69. Article 4 CRD

70. Article 6 CRD

71. Article 9 CRD

72. For example, in Spain companies have to provide the pre-contractual information for consumers in Spanish, in accordance with article 60 Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias - https://www.boe.es/buscar/act.php?id=BOE-A-2007-20555

73. http://ec.europa.eu/consumers/consumer_rights/review/index_en.htm

74. Article 20 Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market

75. Recital 95 Services Directive

76. European Commission staff working document "A Digital Single Market Strategy for Europe - Analysis and Evidence", accompanying the Communication on a Digital Single Market Strategy for Europe, SWD(2015) 100 final, page 24 - http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015SC0100&from=EN

77. Proposal for a Regulation on addressing geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market, COM(2016) 289 final - http://ec.europa.eu/DocsRoom/documents/16742

78. European Commission Communication 'A Digital Single Market Strategy for Europe', COM(2015) 192 final, page 4

79. Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content. http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1450431933547&uri=CELEX:52015PC0634

80. Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the online and other distance sales of goods. http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1450431933547&uri=CELEX:52015PC0635

81. http://ec.europa.eu/consumers/enforcement/cross-border_enforcement_cooperation/index_en.htm

82. Proposal for a Regulation on cooperation between national authorities responsible for the enforcement of consumer protection laws, COM(2016) 283 final. http://ec.europa.eu/consumers/consumer_rights/unfair-trade/docs/cpc-revision-proposal_en.pdf

83. Online dispute resolution platform: https://webgate.ec.europa.eu/odr/main/index.cfm?event=main.home.show&lng=EN

84. European Parliament and Council Directive 99/93/EC of December 13, 1999 on a Community framework for electronic signatures

85. https://ec.europa.eu/digital-single-market/en/digital-single-market

86. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

87. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:en:HTML

88. Payment services directive http://ec.europa.eu/finance/payments/framework/index_en.htm

89. Council Directive 2006/112/EC of November 2006 on the common system of value added tax - http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1464118835088&uri=CELEX:32006L0112

90. VAT rates applied in the Member States of the EU, situation in January 2016, European Commission - http://ec.europa.eu/taxation_customs/resources/documents/taxation/vat/how_vat_works/rates/vat_rates_en.pdf

91. European Commission Communication 'A Digital Single Market Strategy for Europe', COM(2015) 192 final, page 9

92. http://ec.europa.eu/taxation_customs/taxation/vat/how_vat_works/telecom/index_en.htm

93. E-Books: Evolving markets and new challenges, European Parliament, February 2016 - http://ec.europa.eu/taxation_customs/taxation/vat/how_vat_works/telecom/index_en.htm

94. Judgment of the Court of Justice of the European Union of March 5 2015 in cases C-479/13 and C-502/13, Commission v France (http://curia.europa.eu/juris/document/document.jsf?text=&docid=162685&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=415011) and Commission v Luxembourg (http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d54560fbfc457140428451f562707705f3.e34KaxiLc3qMb40Rch0SaxuTa3r0?text=&docid=162692&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=414804)

95. The challenges posed by the necessary interaction between consumer and IP laws can be seen in Australia, for example, where consumer authorities have proposed legislation to authorise the bypassing of illegal geoblocking, which concerned copyright holders. A public consultation is open until June 2016. The Draft Report expressly suggests that the Australian Government should make clear that it is not an infringement of Australia's copyright system for consumers to circumvent geoblocking technology and should seek to avoid international obligations that would preclude such practices. http://www.pc.gov.au/inquiries/current/intellectual-property/draft

96. Directive 2001/29/EC http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001L0029&from=CS

97. Copyright Action Plan: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2015%3A626%3AFIN

98. See EU Commission roadmap http://ec.europa.eu/smart-regulation/roadmaps/docs/2016_cnect_009_cwp_modernising_eu_copyright_2016_en.pdf

99. Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31993L0083

100. In the public consultation document a possible extension to all VOD services is mentioned. However, Martin-Prat's latest intervention mentioned 'only extension to online distribution of TV programmes'.

101. Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights - http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1463746979084&uri=CELEX:32004L0048

102. Article 8 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society - http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1463749364458&uri=CELEX:32001L0029

103. Article 12 et seq. e-Commerce Directive

104. Benzoni, L., The Economic Contribution of the Creative Industries to the EU in terms of GDP and Jobs, TERA Consultants, 2014

105. European Commission Communication 'Towards a modern, more European copyright framework', COM(2015) 626 final - http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=12526

106. Communication on Online Platforms and the Digital Single Market Opportunities and Challenges for Europe. https://ec.europa.eu/digital-single-market/en/news/communication-online-platforms-and-digital-single-market-opportunities-and-challenges-europe

107. European Commission, Special Eurobarometer 431, 'Data protection', 2015 - http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_sum_en.pdf

108. European Commission Communication 'A Digital Single Market Strategy for Europe', COM(2015) 192 final, page 13- http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN

109. Idem

110. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) - http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

111. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data - http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1463056215838&uri=CELEX:31995L0046

112. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) - http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1463056300222&uri=CELEX:32002L0058

113. European Commission Communication 'A Digital Single Market Strategy for Europe', COM(2015) 192 final, page 13

114. Article 4 Data Protection Directive

115. Article 3 GDPR

116. Article 27 GDPR

117. Article 20 GDPR

118. Article 32 GDPR

119. Article 40 et seq. GDPR

120. Article 24 Data Protection directive

121. See Information Commissioner's Office (ICO) guidance about the issue of monetary penalties prepared and issued under section 55C (1) of the Data Protection Act 1998 - https://ico.org.uk/media/1043720/ico-guidance-on-monetary-penalties.pdf and ICO Framework used to guide ICO staff in determining the appropriate amount of a monetary penalty - https://stewartroom.co.uk/wp-content/uploads/2014/08/UK-ICO-Framework-for-amount-of-MP-April-2013.pdf

122. Article 83 GDPR

123. http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2013/notas_prensa/common/diciembre/131219_PR_AEPD_PRI_POL_GOOGLE.pdf

124. Article 56 GDPR

125. Article 60 GDPR

126. Article 63 et seq. GDPR

127. Article 68 GDPR

128. Article 52 GDPR

129. Article 58 GDPR

130. http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

131. "Creation of a global culture of cybersecurity and the protection of critical information infrastructures". http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf

132. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

133. https://www.enisa.europa.eu/

134. https://www.europol.europa.eu/ec3

135. NIS Directive http://data.consilium.europa.eu/doc/document/ST-5581-2016-REV-1/en/pdf

136. European Commission Joint Communication on Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyberspace, JOIN(2013) 1 final - https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

137. https://ec.europa.eu/digital-single-market/en/cybersecurity-industry

138. Gartner IT Glossary http://www.gartner.com/it-glossary/big-data/

139. European Commission Communication 'A Digital Single Market Strategy for Europe', COM(2015) 192 final, page 14

140. European Commission staff working document "Advancing the Internet of Things in Europe", accompanying the communication on Digitising European Industry – Reaping the full benefits of a Digital Single Market, SWD(2016) 110/2, page 59 - https://ec.europa.eu/digital-single-market/en/news/staff-working-document-advancing-internet-things-europe https://ec.europa.eu/digital-single-market/en/news/staff-working-document-advancing-internet-things-europe

141. European Commission Communication 'Towards a thriving data-driven economy', COM(2014) 442 final - https://ec.europa.eu/digital-single-market/news/communication-data-driven-innovation

142. http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm

143. European Commission Communication 'A Digital Single Market Strategy for Europe', COM(2015) 192 final, page 15

144. The Digital Economy & Society Index (DESI) - https://ec.europa.eu/digital-single-market/en/desi

145. Final Report of the study "SMART 2013/0043 – Uptake of the Cloud in Europe" - https://ec.europa.eu/digital-single-market/en/news/final-report-study-smart-20130043-uptake-cloud-europe

146. European Commission Communication 'A Digital Single Market Strategy for Europe', COM(2015) 192 final, page 15

147. Idem

148. European Commission Communication 'Unleashing the Potential of Cloud Computing in Europe', COM(2012) 529 final - http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF

149. https://ec.europa.eu/digital-single-market/en/cloud-computing-strategy-working-groups

150. https://ec.europa.eu/digital-single-market/en/news/cloud-service-level-agreement-standardisation-guidelines

151. The code is currently being reworked in line with the recommendations made by European data protection authorities October 2015 - http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf

152. See section on Cybersecurity

153. Article proposal for a Directive on contracts for the supply of digital content - http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1450431933547&uri=CELEX:52015PC0634

154. Study "SMART 2013/0037 – Cloud and IoT combination"

155. European Commission Communication 'A Digital Single Market Strategy for Europe', COM(2015) 192 final, page 15

156. European Commission staff working document "Advancing the Internet of Things in Europe", accompanying the communication on Digitising European Industry – Reaping the full benefits of a Digital Single Market, SWD(2016) 110/2 - https://ec.europa.eu/digital-single-market/en/news/staff-working-document-advancing-internet-things-europe https://ec.europa.eu/digital-single-market/en/news/staff-working-document-advancing-internet-things-europe

157. European Commission Communication 'ICT Standardisation Priorities for the Digital Single Market' COM(2016) 176 final - https://ec.europa.eu/digital-single-market/en/news/communication-ict-standardisation-priorities-digital-single-market

158. https://www.fiware.org/

159. Horizon 2020 Work Programme 2016-2017:Internet Of Things Large Scale Pilots. https://ec.europa.eu/digital-single-market/en/news/horizon-2020-work-programme-2016-2017-internet-things-large-scale-pilots

160. BEREC: enabling the Internet of Things – Feb. 2016. http://berec.europa.eu/files/document_register_store/2016/2/BoR_%2816%29_39__BEREC_IoT_Report_FINAL_for_publication.pdf

161. http://iotbusinessnews.com/2015/11/25/52013-latin-america-to-reach-159-million-machine-to-machine-iot-connections-by-2024/

162. Communication on a European agenda for the collaborative economy, June 2, 2016. http://ec.europa.eu/DocsRoom/documents/16881

163. Until now, Member States have taken divergent approaches towards the collaborative economy

164. Regulated access to the local loop and bitstream access was imposed in Brazil on fixed incumbent telcos in 2012 under the General Competition Plan - PGMC (Anatel Resolution 600/2012). The PGMC excludes fibre access networks under the scope until 2021. Alternative operators have shown no significant interest in copper-based LLU or bitstream access. In Mexico the regulator IFT imposed unbundled access to América Móvil, including on fixed telecommunications networks of the incumbent Telmex in 2014. The obligation was imposed as a consequence of América Móvil's designation as 'preponderant' agent in the Telecommunications market. Unbundling rules and the first reference offer were approved by IFT, and published by Telmex, in November 2015. No statistics have been published so far on the demand for unbundled access in Mexico. No regulated LLU or bitstream access services are available in the other major Latin American countries.

165. Regulation (EC) No 2887/2000 of the European Parliament and of the Council of 18 December 2000 on unbundled access to the local loop.

166. No public data available for Bolivia, Paraguay, and Venezuela

167. Platform breakdown was estimated by Cullen Intenational based on 2013 data, as no technology breakdown was published by the regulator for 2014.

168. https://pt-br.facebook.com/business/news/BR-45-da-populacao-brasileira-acessa-o-Facebook-pelo-menos-uma-vez-ao-mes

169. GSMA, Roaming Services in Latin America (2013) http://www.gsma.com/latinamerica/roaming-services-in-latin-america

170. ITU, GSR discussion document: the impact of taxation on the digital economy, 2015 https://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2015/Discussion_papers_and_Presentations/Discussionpaper_taxation.pdf
ITU also indicates international roaming as one of the priority issues to be analysed and addressed in future legislative or regulatory measures in its Reporte Post Cumbre Concectar Las Americas 2015. https://www.itu.int/en/ITU-D/Conferences/connect/Documents/Post%20Connect%20Americas%20Summit%20Report%20%28Spanish%29.pdf

171. Source: Subtel http://www.subtel.gob.cl/paises-mas-conectados-de-latinoamerica-acuerdan-estudiar-el-roaming-internacional/

172. July 2014 http://www.prensario.net/9743-Argentina-y-Chile-acuerdan-eliminacion-del-roaming-internacional.note.aspx

173. UNASUR's members are 12 South American countries http://www.unasursg.org/es/estados-miembros

174. http://www.unasursg.org/node/152

175. El ecosistema y la economía digital en América Latina (Raúl Katz, 2015) http://scioteca.caf.com/handle/123456789/768

176. The average Latin American Internet user spends 21.7 hours/month connected. The average European user spends 25.1 hours/month and the average North American 35.9 hours/month. The world average user of social media dedicates 63.55% of the connected time to social media activities. Latin Americans dedicate 78.42% of their time in the Internet for social media activities.

177. The study's estimates only consider the value generated by online platforms, excluding the costs of the products and services sold, advertising and delivery (page 83).

178. IDC for PayPal (2014), partially made public by Camara-e.net Brazil http://www.camara-e.net/2015/06/10/america-latina-um-mercado-em-crescimento-para-o-ecommerce

179. A study by CEPAL/Fundación Telefónica (Katz, 2015) shows that Latin America had over 284.6m Internet users at the end of 2013, i.e. 46,7% of its population. The number of users grew on an average by 10.52% yearly from 2010, with Chile, Colombia, Mexico and Venezuela in the lead.

180. Paypal cross-border research 2014 – snapshot https://www.paypalobjects.com/webstatic/en_US/mktg/pages/stories/pdf/paypal_cbt_global_snapshot_nov_2014_2.pdf

181. América Latina, um mercado em crescimento para o e-commerce, July 2015. http://www.camara-e.net/2015/06/10/america-latina-um-mercado-em-crescimento-para-o-ecommerce

182. A concrete example concerns eDreams, the Spanish online travel agency, not present in Brazil. The local company responsible for the registration of www.edreams.com.br was made liable in several lawsuits and complaints made by consumers to the consumer protection entity PROCON.

183. Full members of Mercosur are Argentina, Brazil, Paraguay, Uruguay and Venezuela. Chile, Colombia, Peru and Ecuador are associate members. Bolivia is an acceding member. Mexico and New Zealand are observers.

184. The e-signature project was cofounded with EU funds of €7m (Mercosur countries investments totalled €3.5m). Source: http://www.camara-e.net/2013/10/23/projeto-mercosul-digital-novo-cenario-para-a-economia-digital-no-mercosul/

185. Argentina, Brazil, Chile, Peru and Uruguay are associate members of the Andean Community. Mexico and Panama are observers.

186. Andean Community website. http://www.comunidadandina.org/Prensa.aspx?id=3263&accion=detalle&cat=AF&title=expertos-gubernamentales-de-paises-de-la-can-definenproyecto-de-norma-sobre-certificados-de-origen-digital

187. TPP Latin American members are Peru, Mexico and Chile. Colombia has expressed an interest in entering the agreement in the past.

188. https://www.mfat.govt.nz/assets/_securedfiles/trans-pacific-partnership/text/14.-electronic-commerce-chapter.pdf

189. With the only exception of Peru, which is a member of both the Andean Community and of the TPP

190. http://www.gsma.com/mobilefordevelopment/programme/mobile-money/state-of-the-industry-2015

191. International Publishers Association, VAT/GST on Books & E-books. (2015). http://www.internationalpublishers.org/images/VAT2015.pdf

192. http://reports.weforum.org/global-competitiveness-report-2015-2016/

193. The ICMS Tax is imposed at state level on the consumption of goods and services. It is similar to the VAT, and varies from 25% to 33% depending on Brazilian states

194. GSR discussion paper The Impact of taxation on the digital economy, ITU 2015 https://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2015/Discussion_papers_and_Presentations/Discussionpaper_taxation.pdf

195. Aimed at starting a dialogue to define public policies for the development of the Latin American digital ecosystem, in 2015 CAF – Development Bank of Latin America, the Economic Commission for Latin America and the Caribbean (ECLAC), the Centre for Latin American Telecommunication Studies (cet.la) and the Fundación Telefónica carried out the study 'The Digital Ecosystem and Economy in Latin America'.

196. AHCIET and Deloitte, Taxation and Telecommunications in Latin America. (2012).

197. GSMA and Deloitte, Mobile telephony and taxation in Latin America. (2012). http://www.gsma.com/publicpolicy/wp-content/uploads/2012/12/GSMA-2012-Latin-America-Tax-ReportWEBv2.pdf

198. IIRSA, South American Roaming Regional Study. (2008). http://www.iirsa.org/admin_iirsa_web/Uploads/Documents/tid_presentacion_estudio_roaming_eng.pdf

199. Regulatel, Double Taxation of VAT on Roamig Services in the Americas Region. (2013). http://www.regulatel.net/roaming/images/Estudios/Bitributacion.pdf

200. The Andean Community is a customs union comprising Bolivia, Colombia, Ecuador, and Peru. Until 1996, it was called the Andean Pact, which came into existence when the Cartagena Agreement was signed in 1969.

201. Decision No. 351 Establishing the Common Provisions on Copyright and Neighboring Rights http://www.wipo.int/wipolex/en/text.jsp?file_id=223494

202. Law 9.610/98. Art. 81. The authorisation from author and performer of a literary, artistic or scientific work for its adaptation to an audiovisual work implies, unless otherwise agreed, the consent to its economic exploitation. § 1º The exclusivity of the authorisation demands an express clause and will cease after ten years of the celebration of the agreement.

203. Falta nota

204. Latin America and the Caribbean is the region with the lowest rate of local content, with 26.60% in 2013. The Middle East and North Africa has a percentage of 27.20%. On the other hand, the rate for the USA is 57.79% and Russia leads with 67.22%. See Katz (2015, p. 78).

205. http://abpitv.com.br/site/secretaria-do-audiovisual-do-minc-mostra-projetos-para-2016-dando-espaco-para-vod-e-mercado-de-games/

206. CACI (Conferencia de Autoridades Cinematográficas de Iberoamérica) is a regional organisation, specialised in audiovisual and cinema. Created in 1989 by the signing of the Iberoamerican cinematographic integration Convention, it is composed of the main audiovisual authorities of 21 countries, including: Argentina, Bolivia, Brazil, Colombia, Costa Rica, Cuba, Chile, Ecuador, El Salvador, Spain, Guatemala, Mexico, Nicaragua, Panama, Paraguay, Peru, Portugal, Puerto Rico, the Dominican Republic, Uruguay and Venezuela.

207. The VOD platform is primarily available for educational and cultural institutions only.The programme's members are from 19 countries: Argentina, Bolivia, Brazil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Spain, Guatemala, Mexico, Panama, Paraguay, Peru, Portugal, Puerto Rico, the Dominican Republic, Uruguay and Venezuela. For more information: http://www.programaibermedia.com/etiqueta/doctv-latinoamerica/

208. http://www.alianza.tv/files/NetnamesAlianzaReport012016.pdf

209. http://www.alianza.tv/files/CP_AlianzaNetNames_210116.FINALVERSION.pdf

210. In 2012, the Ministry of Culture sent the final version of the project (not public) for President's ratification, with no outcome yet. In 2013, a reform was passed (Law 12.853/13) directed only towards regulating the role of societies responsible for collecting levies on music works.

211. Law 17336 as amended in 2010 https://www.leychile.cl/Navegar?idNorma=28933

212. Mercosur Parliament approved a Protocol for the Harmonisation of Intellectual Property (1995), covering trademarks, geographical indications and designation of origins. Another Protocol (1998) covered industrial designs. Discussions on a further Protocol for the harmonisation of copyrights and neighbouring rights were last documented in 2006 and no agreement has yet been achieved. In 2006, the bloc approved the allocation of resources from Fondo Mercosur Cultural to the development and the circulation of cultural services as a means to enhance regional integration. No specific action to fight online piracy is discussed or included in the public documents.

213. For more information: https://ustr.gov/acta

214. A cooperation between Mercosur-UNASUR agreed on the creation of a joint Technical Committee on illegal trafficking of cultural goods, in October 2015. This initiative, however, targets only cultural goods (such as museum pieces and articles found during illegal excavations) and does not yet concern digital goods or online piracy.

215. http://www.oas.org/juridico/spanish/cybersp.htm

216. Bogota, 2015 http://www.oas.org/en/sla/dlc/remja/pdf/remja_x_rec_conc_en.pdf

217. More information at: http://conferenciaelac.cepal.org/sites/default/files/15-00757_elac_digital_agenda.pdf

218. More information at: http://www.oas.org/en/sla/dil/newsletter_data_protection_IAJC_report_Apr-2015.html

219. The OECD Privacy Framework is available at: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

220. The APEC Privacy Framework is available at: https://cbprs.blob.core.windows.net/files/APEC%20Privacy%20Framework.pdf

221. More information at: http://www.oas.org/en/sla/dil/docs/CJI-doc_474-15_rev2.pdf

222. Idem

223. Available at: http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378

224. Idem.

225. The Court issued the final ruling in Schrems v. Data Protection Commissioner (Case C-362/14) on 6 October 2015. Available at: http://curia.europa.eu/juris/celex.jsf?celex=62014CJ0362&lang1=en&type=TXT&ancre=

226. More information at: http://inicio.inai.org.mx/nuevo/Observaciones%20INAI%20a%20proyecto%20de%20dictamen%20LGPDP.pdf

227. More information at: http://www.sic.gov.co/drupal/noticias/claves-para-entender-el-RNBD

228. OAS: Adoption of a comprehensive Inter-American strategy to combat threats to cybersecurity: a multidimensional and multidisciplinary approach to creating a culture of cybersecurity https://www.oas.org/en/sms/cicte/Documents/OAS_AG/AG-RES_2004_%28XXXIV-O-04%29_EN.pdf

229. Argentina's national programme on critical infrastructure and cybersecurity. http://www.infoleg.gov.ar/infolegInternet/anexos/185000-189999/185055/norma.htm

230. Law 26388/2008 http://www.infoleg.gov.ar/infolegInternet/anexos/140000-144999/141790/norma.htm and Law 26904/2013 http://www.infoleg.gob.ar/infolegInternet/anexos/220000-224999/223586/norma.htm

231. Law 1273 of 2009 http://www.mintic.gov.co/portal/604/w3-article-3705.html

232. Cybersecurity and cyberdefense guidelines from the National Council on economic and social policy within the National Planning Department http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

233. The proposal of a new law was expected to be presented in March 2016, in an OECD meeting. http://www.welivesecurity.com/la-es/2016/02/01/chile-ley-de-proteccion-de-datos-personales/

234. Chamber of Deputies PL 5276/2016 http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378

235. Frost&Sullivan. Reference available at: http://www.telesintese.com.br/investimento-em-nuvem-publica-crescera-153-em-3-anos-na-america-latina/

236. A hybrid cloud is based on a partially public, partially private infrastructure

237. Decree 8.135/2013 (https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d8135.htm) regulated by MP/MC/MD 141/2014 (https://www.legisweb.com.br/legislacao/?id=269793)

238. Ministry of Planning: Boas práticas, orientações e vedações para contratação de Serviços de Computação em Nuvem', http://www.planejamento.gov.br/assuntos/logistica-e-tecnologia-da-informacao/noticias/computacao-em-nuvem-dados-devem-permanecer-no-brasil

239. https://www.gsmaintelligence.com/research/2015/05/m2m-in-latin-america-state-of-the-market/506/

240. Law 12715/2012 http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12715.htm

241. Presidential decree 8234/2014 http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/Decreto/D8234.htm

242. Data section in Anatel website: http://www.anatel.gov.br/dados/index.php/destaque-1/283-movel-acessos-maio

243. Portaria 2006/2016 http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=12/05/2016&jornal=1&pagina=149&totalArquivos=248

244. BNDES, Public call for tender of 2016 http://www.bndes.gov.br/SiteBNDES/bndes/bndes_pt/Institucional/Apoio_Financeiro/Apoio_a_estudos_e_pesquisas/BNDES_FEP/prospeccao/chamada_internet_das_coisas.html

245. Brasil Inteligente Programme, published by decree 8776/2016 just before president Dilma Rousseff was suspended http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8776.htm

246. Ministry of Justice of Argentina: Guidelines on best practices regarding privacy in the development of applications (http://infoleg.mecon.gov.ar/infolegInternet/anexos/245000-249999/245973/norma.htm)

247. CADE, Working document 3/2015 http://www.cade.gov.br/acesso-a-informacao/publicacoes-institucionais/dee-publicacoes-anexos/rivalidade-apos-entrada-o-impacto-imediato-do-aplicativo-uber-sobre-as-corridas-de-taxi.pdf

248. City Hall, Decree 56981/2016 http://diariooficial.imprensaoficial.com.br/nav_cidade/index.asp?c=1&e=20160511&p=1&clipID=0PA1DJRUPIG02e9IF2Q0OLFVCA9

249. Law 5691/2016 (http://www.buriti.df.gov.br/ftp/diariooficial/2016/08_Agosto/DODF%20148%2003-08-2016/DODF%20148%2003-08-2016%20SECAO1.pdf)

250. Available at: http://www.oas.org/dil/treaties_A-41_Charter_of_the_Organization_of_American_States.htm

251. CITEL RES. 70 (VI-14): https://www.citel.oas.org/en/SiteAssets/About-Citel/CITEL%20STRATEGIC%20PLAN%202014-2018_i.pdf

252. Works were carried out from 2005, and in the respective Action Plans were adopted In Rio de Janeiro, and then at the Ministerial Conferences of San Salvador (2008), Lima (2010), Montevideo (2013), Mexico City (2015).

253. This ECLAC report has been used for the preparatory phase of the eLAC 2018 Plan of Action. http://repositorio.cepal.org/bitstream/handle/11362/38767/S1500587_en.pdf?sequence=1

254. Red Clara http://www.redclara.net/index.php/en/

CAF DEVELOPMENT BANK OF LATIN AMERICA