Key findings of the Internet & Jurisdiction and ECLAC

Regional Status Report 2020

UNITED NATIONS

ECLAC

INTERNET & JURISDICTION
POLICY NETWORK

german
cooperation
DEUTSCHE ZUSAMMENARBEIT

Thank you for your interest in this ECLAC publication

Please register if you would like to receive information on our editorial products and activities. When you register, you may specify your particular areas of interest and you will gain access to our products in other formats.

Register

UNITED NATIONS

ECLAC

www.cepal.org/en/publications

facebook.com/publicacionesdelacepal

www.cepal.org/apps

This document sets forth the key findings of the report commissioned by the Secretariat of the Internet & Jurisdiction Policy Network (I&JPN) and the United Nations Economic Commission for Latin America and the Caribbean (ECLAC). The document was authored by Carlos Affonso de Souza.

The report represents the best endeavour to map the current ecosystem and trends based on desk research, as well as stakeholder surveys and interviews. The completeness of information cannot be guaranteed, however, as this report constitutes a first regional baseline on the state of jurisdiction on the Internet.

ECLAC and the Secretariat of the Internet & Jurisdiction Policy Network are grateful for the financial and institutional support of Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ), on behalf of the German Federal Ministry for Economic Cooperation and Development (BMZ), which has enabled the production of this report.

United Nations publication
LC/TS.2020/68
Distribution: L

Printed at United Nations, Santiago
S.20-00402

Internet & Jurisdiction Policy Network publication

This publication should be cited as: Economic Commission for Latin America and the Caribbean (ECLAC) / Internet & Jurisdiction Policy Network (I&JPN), *Key findings of the Internet & Jurisdiction and ECLAC Regional Status Report 2020* (LC/TS.2020/68), Santiago, 2020.

CONTENTS

FOREWORD

The digital transformation of economies, governments and societies in Latin America and the Caribbean is sharply accelerating in 2020, further catalysed by the COVID-19 pandemic. With the growth of cross-border services and data flows, the need for more legal interoperability and coordination rises. Uncoordinated action of a wide range of actors and initiatives risk hampering the digitalisation. To provide an indispensable mapping and analysis of the regional ecosystem in Latin America and the Caribbean, the Internet & Jurisdiction Policy Network in coordination with the United Nations Economic Commission for Latin America and the Caribbean created this first Internet & Jurisdiction and UN ECLAC Regional Status Report 2020. It is a regional edition of the groundbreaking Internet & Jurisdiction Global Status Report 2019. The Report builds on the unique methodology of the Internet & Jurisdiction Policy Network to mutualize knowledge of key stakeholders from states, companies, technical operators, international organizations, academia and civil society through interviews and surveys.

A key message of the Regional Status Report is that more policy coherence is needed to build a thriving and integrated regional digital ecosystem. By laying out key trends with regard to the handling of legal challenges on the continent, the Report is intended to allow policy makers and shapers to enhance their understanding of the myriad of fast-paced developments to enable evidence-based policy innovation and advance legal interoperability in cyberspace. Bridging the fields of the digital economy, security and human rights, the Report sheds light on the changing technological and regulatory landscape in the region. It provides the most up-to-date overview of the plurality of national and private policy initiatives, as well as jurisprudence that sets the rules for online interactions, digital services and data flows. The Report reveals the latest trends on key topics ranging from start-ups, artificial intelligence, Internet of Things, expression, and privacy to the role of intermediaries. Moreover, it showcases the geographic extension and impact of national measures from the region, as well as the influence of public and private regulatory measures from outside of it.

This important mapping for policy and decision makers was created thanks to the strong partnership between the Internet & Jurisdiction Policy Network and UN ECLAC under the five-year Memorandum of Understanding signed in 2019. The Regional Status Report is an important milestone in the efforts of the Internet & Jurisdiction Policy Network to map the global cross-border legal ecosystem to help develop better policies and solutions. We therefore hope that it can contribute to fostering coordination on cross-border legal challenges and digital cooperation in Latin America and the Caribbean, and beyond.

Bertrand de La Chapelle
Executive Director

Paul Fehlinger
Deputy Executive Director

Secretariat of the Internet & Jurisdiction Policy Network

As Latin America and the Caribbean battles the most severe health and humanitarian crisis in a century, the inequalities that pervade the region have been laid bare. Just as the coronavirus disease (COVID-19) pandemic has revealed the consequences of unequal access to health care, a high-quality education system and economic opportunities, the stark digital divide has also become more evident. Over 60% of individuals in the region have an Internet connection, but there are marked inequalities in connectivity by income, rural and urban areas and ethnicity, among other factors. In some countries, the connectivity gap between the richest and poorest quintiles is as wide as 60 percentage points. To weather the crisis and build back better, it is essential that steps be taken to move towards universal connectivity and provide greater access to digital tools. This will only be possible with strong normative frameworks.

The COVID-19 pandemic amplifies the need for greater coordination to ensure policy coherence among the countries of the region on issues such as cross-border data transfers, regulatory harmonization, privacy and data security. The deployment of technologies that require the rapid transfer of large amounts of new data among numerous actors to control the spread of COVID-19 calls for common standards and legal interoperability. The increased importance of remote working and distance-learning initiatives requires secure connectivity solutions to ensure no one is left behind.

As the technical secretariat of the Ministerial Conference on the Information Society in Latin America and the Caribbean, the Economic Commission for Latin America and the Caribbean (ECLAC) has been working in coordination with government stakeholders and observer representatives from academia, industry, the technical community and multilateral organizations to prepare a regional digital agenda, prioritizing issues related to the digital development of our region for over 15 years. As we develop the 2020–2022 digital agenda for Latin America and the Caribbean (eLAC2022), one of the highest priority initiatives is the creation of a regional digital market. The regional digital market seeks to strengthen the digital integration of Latin America and the Caribbean, taking advantage of the geographical proximity and similar interests of the region's countries.

This pioneering report is the first comprehensive mapping of its kind in Latin America and the Caribbean and provides a robust evidence base that will support the development of eLAC2022. The report identifies and addresses key trends in the rapidly growing regional digital policy field and charts the path to be followed. This vital contribution to the policy debate will shed light on some of the challenges we face and opportunities we can seize to bring us closer to a more integrated and harmonized regional digital market.

Alicia Bárcena

Executive Secretary
Economic Commission for Latin America and the Caribbean (ECLAC)

METHOD

The method chosen for this Report has been shaped by the need to ensure a comprehensive understanding of a highly complex and dynamic ecosystem —one comprised of multiple actors, initiatives and trends across the policy silos of the digital economy, human rights and security.

This has led to the adoption of a flexible, qualitative research design that enables an in-depth exploration of the research questions. By using the multifaceted research method first adopted for the production of the pioneering Internet & Jurisdiction Global Status Report 2019, this Report incorporates an unprecedented and innovative large-scale collaborative contribution and review process in the Latin America and the Caribbean (LAC) region.

This process leveraged the combined expertise of the key stakeholders engaged in the Internet & Jurisdiction Policy Network and UN ECLAC and beyond through semi-structured interviews, peer review feedback and data collection procedures, combined with detailed and extensive desk research.

The desk research

Desk research adopted conventional legal research methods and consisted primarily of a comprehensive study and analysis of relevant case law, legislation and other regulatory initiatives, as well as the literature —including books, journal articles, published conference papers and industry publications. This was supplemented with a detailed study of a variety of valuable reports and other materials from a range of bodies over recent years.

The desk research benefited greatly from publications produced by UN ECLAC and the Internet & Jurisdiction Policy Network's wide-ranging collection of relevant developments available in the I&J Retrospect Database. The Retrospect Database is the flagship, open-access publication of the Internet & Jurisdiction Policy Network, documenting policy developments, judicial decisions, international agreements and other cases that reflect jurisdictional tensions on the cross-border internet. This important collection provided up-to-date insights into current major trends, attitudes, developments and initiatives. The materials contained in the Retrospect Database also provided important insights into current legal and technical approaches to solutions, as well as to what this Report defines as 'overarching trends'.

The stakeholder survey

The first method for gaining stakeholder input consisted of an online survey made up of 15 questions on a variety of topics relevant for the research questions. In considering how best to gather survey data to inform the research questions, great care was taken to design questions that may be answered by any of the relevant stakeholders. This ensured that all survey participants were exposed to the same set of questions. The Internet & Jurisdiction Policy Network Secretariat and UN ECLAC identified survey participants representing all of I&JPN's stakeholder groups —i.e., academia, civil society, governments, international organizations, internet platforms and the technical community— and participants were specifically selected to guarantee geographical diversity in the LAC region. Furthermore, the selection of the survey participants was purposive, in that they were specifically targeted based on their considerable expertise and knowledge. In total, input was received from over 40 survey participants during a period from Q4 2019 - Q2 2020. Participants provided their views in their personal capacity, rather than as representatives of any specific organization. Furthermore, input gained from the surveys has only been used without attribution. The expert input gained from the survey was invaluable. Apart from bringing attention to major topical trends, approaches to solutions, overarching trends and generally held concerns in the ecosystem, the survey results helped provide both context and a more nuanced understanding of the operating environments facing civil society, governments, international organizations, internet platforms and the technical community. Survey results are used throughout the Report to show, in figures, the concerns and attitudes of the surveyed stakeholder ecosystem. In addition, the comments from surveyed stakeholders are used to highlight particularly important arguments, observations and concerns.

Stakeholder interviews

Semi-structured interviews were organized across a broad range of stakeholders in order to complement the insights gained from the survey responses and desk research. As with the surveys, great care was taken to ensure inclusiveness and diversity, with the selected interviewed experts representing academia, civil society, governments, international organizations, internet platforms and the technical community, with geographical diversity. These stakeholders were identified both from within and outside the Internet & Jurisdiction Policy Network and UN ECLAC.

Each interview lasted over 30 minutes, on average. The interviews were conducted in confidence and as such, were not recorded. Detailed notes were collated, however, and observations were recorded in a structured manner, facilitating cross-referencing and detailed analysis. The semi-structured interviews allowed for considerable flexibility and catered for supplementary questions based on discussions with the interviewee. This —combined with the confidentiality guarantee— provided an environment in which interviewed stakeholders could highlight matters important to them within the topics discussed. In many cases, the interviewees could also provide perspectives, insights and information that might otherwise have been unattainable by researchers. In this way, part of the purpose of the interviews was to reduce regional and topical gaps in the desk research. In total, over 30 interviews were carried out from Q4 2019 to Q2 2020. The interviewed stakeholders provided their views in their personal capacity rather than as representatives of any specific organization. Furthermore, input gained from the interviews has only been used without attribution. Like the comments made by surveyed stakeholders, the interviewed stakeholders' comments were vital and are used throughout the Report to highlight particularly important arguments, observations and concerns.

Limitations of the study

A research study of this nature carries certain limitations. First, the scope of the Report is delineated by reference to the Internet & Jurisdiction Policy Network's and UN ECLAC's mandate. Thus, this is not a Regional Status Report generally about the Internet; rather it is specifically focused on cross-border legal issues in relation to the internet. Second, despite the steps outlined above, the inevitable risk of gaps must be acknowledged. The statistical relevance of exploratory research relying, in part, on a limited number of survey participants and interviewed experts should not be overstated. In addition, most forms of desk research may involve biases that are difficult to eliminate in full in spite of best efforts.

In light of the above, this Report represents a best-effort attempt at painting a broad-brushed, yet comprehensive, overview and documentation of past, current and emerging trends, relevant actors, and proposed solutions to the major cross-border legal policy challenges facing our connected society as of 1 June 2020. As such, it is a timely snapshot of the policy environment and creates a first regional baseline in the LAC region against which future studies may be undertaken.

EXECUTIVE SUMMARY I

The *Internet & Jurisdiction and UN ECLAC Regional Status Report 2020* is the region's first comprehensive exercise to map the different policy trends that revolve around the issue of the trans-border nature of the internet and how it affects different actors such as governments, companies and civil society.

How might different regional and national regulations create barriers that hinder cross-border e-commerce and investment in digital markets? Which economic and social benefits could be reached by the harmonization of frameworks throughout the region? A better understanding of this scenario is a key factor to foster investor confidence, to promote innovation and economic diversification, attracting more confidence in the use of e-commerce and boosting a market of more than 600 million people, while opening several opportunities for businesses and particularly for small and medium enterprises.

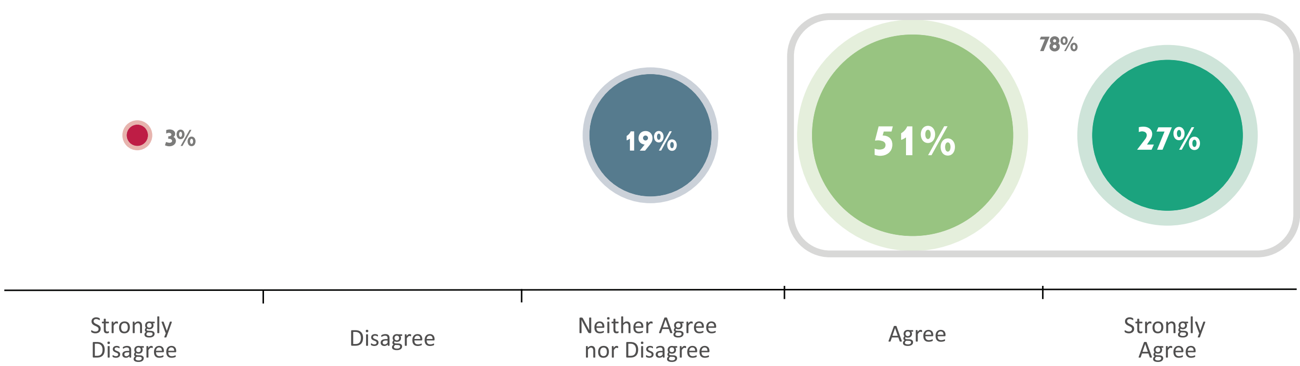
At the same time, uncoordinated action of a wide range of actors and initiatives risk hampering the digitalization of economies, governments, and societies. In order to help policy makers navigate the challenges ahead, the Internet & Jurisdiction Policy Network (I&JPN), in coordination with the United Nations Economic Commission for Latina America and the Caribbean (UN ECLAC), present this Regional Status Report.

The report aims at: (i mapping and consolidating information relevant to the LAC region and the Regional Digital Market; (ii setting up and strengthening regional contributor networks; and (iii developing capacity building for relevant stakeholders on cross-border legal topics associated with the digital transformation.

Throughout surveys and interviews with several leading experts in the region, the report reveals that 78% agree that cross-border legal challenges on the internet will become increasingly acute in the next three years. At the same time, 73,17% of the interviewed stakeholders agree or strongly agree that there is a demand for coordination to address cross-border legal challenges, even as 60,98% believe that we still do not have the right institutions to tackle those challenges.

Figure 1

Will cross-border legal challenges on the internet become increasingly acute in the next three years?



Source: The author.

In an effort to analyze trends that are unique to the region, the report investigates how a changing technological landscape empowers the idea of transnational activities as an emerging new dynamic that involves not only big multinational companies, but that also sets the stage for the accelerated growth of regional startups.

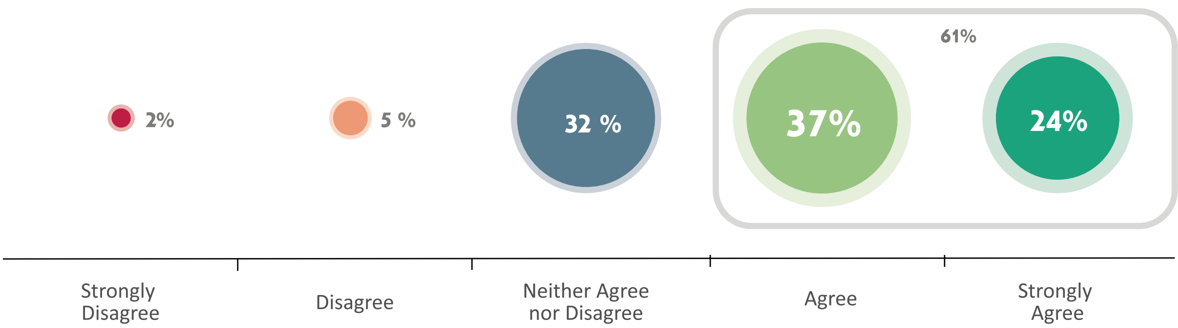
The report identifies how regional and national regulatory frameworks might be inspired by foreign initiatives, especially those arising out of the United States and the European Union. Such is the case of the European General Data Protection Regulation (GDPR), which sparked several legislative changes in the LAC region. Is there any room for cross-fertilization or is it a mere replication?

As major internet companies have to deal with changing expectations from governments and the general public, with increasing demands for more responsibility, a plurality of norms make the region ripe for jurisdictional conflicts, testing the limits of enforceability and the reach of national laws.

The major topical trends in the LAC region are organized in three groups: expression, security and economy. There is no shortage of trends that are unique to the region, even though some of them are also presented on a global scale.

One of the most pressing trends on "expression" is how the fight against disinformation and the so-called fake news is leading many countries to adopt new rules that might have impacts that go way beyond a country's border. 60,98% of the interviewed stakeholders agree or strongly agree that the cross-border nature of the internet facilitates foreign interference with the democratic process. Cases in which automatized social media accounts created abroad end up playing a role in the elections of a different country are not uncommon in the region.

Figure 2
Does the cross-border nature of the internet facilitate foreign interference with the democratic process?



Source: The author.

The very same demand for cooperation among countries to address jurisdictional challenges has surfaced in the region during the investigations of corruption scandals. To produce evidence located in a different country, law enforcement agents in the LAC region are pushing for more cooperation, creating the conditions for standardization of cross-border data transfers in the region.

Coordination is a key element for a LAC Digital Single Market. The economic effects of a regional approach to topics such as the widespread of fintech in the region, with extensive support for innovative regulatory solutions, is a clear message that came out of the report's interviews and surveys. 82,92% of the referred stakeholders agree or strongly agree that the deployment of innovative frameworks, such as regulatory sandboxes, helps foster economic growth.

The report also highlights how significant approaches to solutions in the LAC region might come from the law or from the development of technological tools, such as geo-blocking and content filtering, with all due controversies that such resources might bring.

The *Internet & Jurisdiction and UN ECLAC Regional Status Report 2020* hopes to enable evidence-based policy innovation and to provide all stakeholders with the necessary information to develop frameworks and policy standards for the digital society in the LAC region. The following major observations are covered by this Report:

Major transversal aspects to the trends and solutions:

Overarching Trends

- *The landscape is changing:* we have moved from a past romanticized *tech-euphoria* to a moment of *techlash*, heralded by the rise of disinformation, hate speech and cybercrime (with a *tech-intensive* period recently because of/to fight against the Covid-19 pandemic); transnational interactions are an emerging new dynamic; the influence of multinational companies is strong; and the entrepreneurial environment of regional startups grows.
- *Foreign regulatory initiatives influence regional and national proposals*: there is an increasing appetite to regulate cyberspace, as the proliferation of initiatives attests; but are these legislative and judicial inspirations cross-fertilization or mere imitation?
- *Concern over external influence and increasing normative plurality:* rules are set for —and by— established large international actors; and the role of company norms increases, as their Terms of Service reach "constitutional status" on their digital spaces.
- *Interrogations on the role of territoriality/sovereignty in a global network:* national laws have an increasing geographic reach while countries encounter challenges of enforceability.
- *New roles for intermediaries*: increasing responsibilities are bestowed on private operators

Major topical trends in the LAC region

Expression:

- Fake news and disinformation campaigns are triggering countries in the region to seek regulatory action;
- The non-consensual distribution of sexually explicit media ("revenge porn") knows no border and can perpetuate damages;
- The Google Spain case at the European Court of Justice (ECJ) has sparked a regional debate about the "right to be forgotten": while experts recognize the global scope of the right to be forgotten, regional experience with amnesty laws and the notion of a "right to remember" created a backlash to the enforcement of a general right to be forgotten;

- Defamation cases are triggering debates about cross-border effects of the defense of someone's honor. In addition, defamation is both a civil and a criminal offense in many countries in the region, raising additional questions about how the protection of reputation might restrict freedom of expression (e.g. for journalists and bloggers);
- Governments in the region are imposing stricter rules for content moderation and removal on online platforms.

Security:

- There is a growing need for coordination in cybersecurity efforts to overcome widespread incidents in the region;
- Cross-border cases of corruption in the LAC region have fostered a sophisticated debate over practices of multi-jurisdictional investigations;
- Access to digital evidence in multiple jurisdictions triggers a review of known practices of investigations in the LAC region;
- Regional stakeholders do not advocate for the overhaul of the Mutual Legal Assistance (MLA) system, but instead, support its adaptation to the digital age; yet, law enforcement in the region are increasingly seeking access to data outside the Mutual Legal Assistance Treaty (MLAT) structure;
- Regional stakeholders agree that the Budapest Convention is a step in the right direction to facilitate cross-border investigations, but it does not solve the problems of MLA system;
- Stakeholders reaffirm that "backdoors" would undermine trust in encrypted systems**.**

Economy:

- Inspired by GDPR, countries in the LAC region are creating or improving their national data protection regulations;
- Half of the countries in the region have a specific data protection regulation, but there is room for improvement and coordination to foster a truly regional framework for data protection;
- Regional initiatives are fostering standardization of cross-border data transfers;
- There is a demand for the creation of a Digital Single Market in the region;
- Stakeholders indicated that areas such as consumer and data protection, digital payments, and tax regimes are key for the creation of a Digital Single Market in the region;
- The region features a strong consumer rights culture, providing a relevant basis for the creation of a Digital Single Market;
- Choice of law and choice of forum clauses tend to be frowned upon in e-commerce due to national consumer protection;
- Internet of Things (IoT) knows no border and demands standardization but Stakeholdersexperts are divided on the need for specific regulation for IoT;
- There are several challenges and opportunities for smart cities in the region;
- Smart farming enlarges the set of international players and is a natural move for the region;

- Digital payments developments in the LAC region coexist alongside an unbanked population, lower penetration of international credit cards, an enduring cash culture, and foreign exchange volatilities;
- Fintechs are revolutionizing financial services in the region, but face disparate regulatory treatment at the national level;
- Cross-border jurisdictional aspects are increasingly impacting the activities of fintechs in the region;
- Stakeholders reveal great enthusiasm for the adoption of innovative regulatory solutions, such as regulatory sandboxes;
- Blockchain and cryptocurrencies are viewed as enablers of cross-border trade (and crime).

Major approaches to solutions in the LAC region: Legal Trends

- States are increasingly resorting to an "effects doctrine" in asserting jurisdiction;
- An expansive geographic scope of jurisdiction may not lead to actual enforcement;
- Higher courts in the region have so far refrained from decisions with a global reach;
- National courts are increasingly ordering platforms to takedown, stay-down, and stay-up content posted online;
- In addition to civil liability, countries are increasingly resorting to administrative sanctions to foster compliance with sectorial norms;
- Companies Terms of Service are interlocked with national laws, reinforcing or disputing the status of a user's behavior;
- Impacts of the controversial update of the European Copyright Directive can already be felt in the region;
- Online marketplaces are deploying dispute resolution systems as governments push for co-regulation on the sale of counterfeit goods;
- For the sake of consumer protection, courts in the region tend to not uphold choice of forum and choice of law clauses in Terms of Service of international platforms.

Major approaches to solutions in the LAC region: Tools

- The use of personal data to map and control the Covid-19 pandemic will consolidate the discussion about geo-location technologies in the region;
- Geo-blocking and geo-pricing are raising concerns over antitrust, consumer, and data protection;
- Content filtering is on the rise as countries fight hate speech and disinformation in the region;
- App blocking has changed from a last resort to a common practice in the region, with important potential impacts across borders;
- DNS blocking is ordered by some governments in the region, but it is not a widespread practice
- Internet shutdowns are not common in the region, but might happen during times of social unrest;
- Mandatory data localization is adopted in the region for various reasons, but it raises serious concerns among stakeholders.

INTRODUCTION - WHY A REGIONAL STATUS REPORT?

II

Regional digital integration is an indispensable element to move towards the diversification of regional economies. There is evidence of the enormous potential of intraregional trade to move towards a more knowledge-intensive export basket. In 2018, 54% of the value of intraregional exports consisted of high, medium and low technology manufactures.[1] On the other hand, the rapid growth of cross-border e-commerce provides major opportunities for small and medium enterprises (SMEs) to trade internationally.

In 2019, 155.5 million people in Latin America were expected to buy goods and services online, a significant 22% growth in comparison to 126.8 million in 2016. However, the average annual number of online transactions *per capita* in Latin America in 2016 was lowest in the world, with only 9.2 online transactions per year.[2]

The region has made significant progress in terms of legislation concerning the internet. In 2017 more than 80% of the countries in Latin America and the Caribbean had some type of legislation on electronic transactions and electronic signature and 90% had regulations on intellectual property matters.

These figures highlight the importance of promoting a harmonized legal and regulatory framework to help eliminate the barriers that hinder cross-border e-commerce and investment in digital markets. The harmonization of policy frameworks throughout the region could create significant economic and social benefits that could lead to increased investor confidence and more foreign direct investment, the promotion of innovation and economic diversification. It could also foster confidence in e-commerce and boost a market of more than 600 million people, while opening several opportunities for businesses and particularly for small and medium enterprises.

Handling the coexistence of heterogeneous laws on the cross-border internet is one of the greatest policy challenges of the 21st century. Yet, scalable and coherent policy solutions cannot be developed without a comprehensive understanding of a highly complex and dynamic ecosystem comprised of multiple actors, initiatives and trends across the policy silos of the digital economy, human rights and security.

To advance the regional debate concerning the definition and application of online legislation and catalyze the development of a shared framework, stakeholders need to engage in ongoing dialogues to help understand the challenges and foster coordination of different initiatives and policy proposals. Quality information through relevant research and documentation is key to support decision-making processes and stimulate evidence-based policy innovation.

Uncoordinated action of a wide range of actors and initiatives risk hampering the digitalization of economies, governments, and societies. To provide an indispensable mapping and analysis of the regional ecosystem in Latin America and the Caribbean, the Internet & Jurisdiction Policy Network (I&JPN) in coordination with the United Nations Economic Commission for Latina America and the Caribbean (UN ECLAC) present the current report.

1 https://repositorio.cepal.org/bitstream/handle/11362/44197/5/S1801069_en.pdf.
2 https://www.statista.com/study/14764/e-commerce-in-latin-america-statista-dossier/.

This report is the first regional version of the pioneering Internet & Jurisdiction Global Status Report 2019 that the organization launched November 2019 at the United Nations Internet Governance Forum in Berlin, providing for the first time a global baseline of the cross-border ecosystem of jurisdiction on the internet. The Regional Status Report is based on the proven methodology of the Global Status Report 2019.

The objectives of the *Internet & Jurisdiction and UN ECLAC Regional Status Report 2020* are the following:

Mapping and consolidation of information relevant to the LAC region and the Regional Digital Market: The Report provides - for the first time - a comprehensive, regional overview and documentation of past, current and emerging trends, relevant actors and proposed solutions to the major cross-border jurisdictional policy challenges, which stakeholders are facing in Latin America and the Caribbean.

The report investigates the most relevant trends and policy challenges of the digital society and economy, building in particular upon the findings and issues addressed in the three programs of the I&JPN, including: cross-border access to user data, cross-border content restrictions, and domain suspensions. Moreover, the report examines the most relevant emerging issues and debates that range from topics such as the Internet of Things, digital trade, blockchain, in order to map these upcoming policy challenges.

Set up and strengthening of regional contributor networks: The report provides a consolidated basis for capacity building through knowledge sharing and the facilitation of well-informed decision making. By using an innovative large-scale collaborative contribution and review process, it sets up a regional contributor network and leverages the combined expertise of engaged stakeholders through structured interviews and data collection efforts.

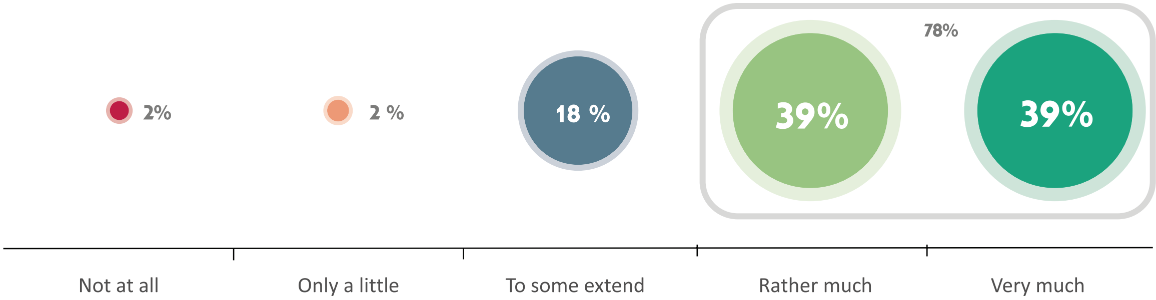
Capacity building for relevant stakeholders on cross-border legal topics associated with the digital transformation: The availability of this comprehensive overview and analysis of trends and initiatives translates the highly complex and often technical nature of substantive issues for decision makers and helps develop an important common taxonomy for the policy ecosystem. The report aims to contribute to the mitigation of acute jurisdictional conflicts, support the development of concrete operational solutions, and equip policy actors with information to prevent losing the benefits of the open, interoperable and cross-border internet.

As the LAC region aims at the development of a Digital Single Market, stakeholders surveyed for this report sent a strong message, with 78,04% agreeing that a significant effort will be required in harmonizing norms to enable this goal. As one of the surveyed experts highlights:

"I believe MERCOSUL and LATAM countries should find a way to engage in a broad cross-border regulation, which could foster the digital economy in the region. Today, the legal framework is very sparse, without a common ground. This unevenness is compromising the region's development."

In a world that transitions toward a new decade, countries in the LAC region are faced with the opportunity to foster regional integration when there is a need for countries to reinvent their roles on the global stage after the Covid-19 pandemic. The social and economic repercussions will be severe and to understand how different policy decisions about the internet (and technology as a whole) might affect other countries will be key to the new frameworks that might arise from the crisis.

Figure 3
How much harmonization of norms would be required to enable a Digital Single Market in the region?

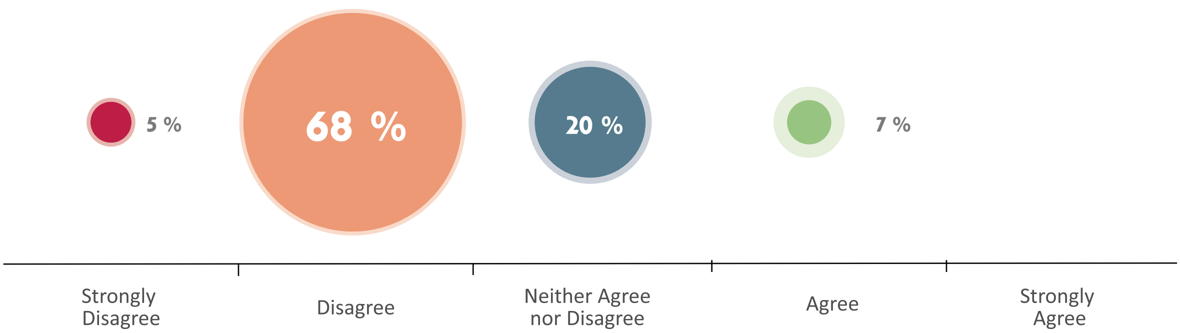


Source: The author.

73,17% of the interviewed stakeholders agree or strongly agree that there is a demand for coordination to address cross-border legal challenges. This number alone sets the direction that this report aims to follow.

This document ("Key Findings") is a compressed and preliminary version of the Internet & Jurisdiction and UN ECLAC Regional Status Report 2020. It serves as a roadmap for practitioners for some of the most pressing issues concerning policy making and the cross-border nature of the internet.

Figure 4
Is there sufficient international coordination and coherence to address cross-border legal challenges on the internet?



Source: The author. the author.

III OVERARCHING TRENDS

The combination of detailed desk research and stakeholder input —via the survey and interviews— drew attention to several overarching trends that are central to any discussion of the cross-border legal challenges on the internet as a whole. Some of these trends are clearly reflective of those showcased in the Internet & Jurisdiction Global Status Report 2019[3], and this report highlights how these trends are specifically developing in the LAC region. These overarching trends are shaping topical trends (Section IV), and to a degree, they are setting the parameters within which the legal and technical approaches may be explored (Section V).

A. The changing technological landscape

If the internet is to connect us all, some argued that no regulation whatsoever should be permitted in cyberspace. Back in 1996, the well-known "A Declaration of the Independence of Cyberspace", by John Perry Barlow, drew a line between the states as "weary giants of flesh and steel" and cyberspace[4] as "the new home of Mind". By stating the virtues arising out from the existence of a virtual space for the free flow of information, Barlow urged states not to interfere with the development of the network through regulations of any kind.

Regulation comes in many different forms, and a state-imposed law is not the only way in which behavior might be stimulated or hindered. Lawrence Lessig, in 1999, suggested that this regulatory tug-of-war could be more complex when it comes to addressing how technology impacts human behavior. Legal rules were not to be the sole source of regulation. Instead, they would dispute space with competing forces such as the market and its economic logic, social constrictions and, finally, technology itself, which could either allow or prohibit a behavior by means of architecture.[5]

The scenario drawn by Lessig reveals that a change in architecture could be more effective than a change in the legislation when it comes to shaping human relations and behavior. "Code is Law" thus became a repeated mantra in the debates over the future of internet regulation.

This debate over internet regulation has changed from the late 90s. On very general terms, the tech-euphoria times of Barlow gave space to a grimmer perception on how internet might be used to commit crimes and to spread disinformation, with a notorious impact on the enjoyment of fundamental rights and the erosion of the political discourse. What had started out as tech-euphoria has turned into "techlash", with significant regulatory efforts.

The beginning of the 2020s however sets an important milestone. As the fight against Covid-19 has forced countries to close borders and impose lockdowns, it was the internet that served as a lifeline for families, businesses and governments to continue

3 https://www.internetjurisdiction.net/news/release-of-worlds-first-internet-jurisdiction-global-status-report.

4 BARLOW, John Perry. "A Declaration of the Independence of Cyberspace" (February 8, 1996). Available at: https://www.eff.org/pt-br/cyberspace-independence.

5 LESSIG, Lawrence. "The Law of Horse; what CyberLaw might teach", in Harvard Law Review v.113, n. 501. Available at: https://cyber.law.harvard.edu/works/lessig/finalhls.pdf.

to communicate during challenging times. We cannot return to the tech-euphoria period, but the pendulum seems to be moving again and the public perception about the role the internet plays in peoples' lives might also suffer another transformation.[6]

As paradoxical as it may seem, the closure of the borders to contain the virus was matched with an increased level of activity by individuals, companies and authorities online. If it is true that the internet turned the transnational into an emerging new dynamic, our shared experiences during the pandemic have reaffirmed that conclusion.

The borderless nature of the internet has created the perfect environment for ideas to reach a wider audience. For entrepreneurship, countries in the LAC region serve as proving ground for numerous inventive solutions to the most diverse challenges. For large multinationals and promising startups, the region continues to offer many opportunities.

However, the feasibility of these opportunities is sometimes dependent on the national and regional regulatory framework. Deciding how to mix foreign inspiration with regional innovation is the first step to understand how to tackle internet policy in the LAC region.

B. Foreign regulatory initiatives influence regional and national proposals

Stakeholders overwhelmingly agree that foreign regulatory approaches impact regional and national initiatives on internet governance and regulation.

While the internet was not designed with countries' borders in mind, regulation of the network has impact far beyond the frontiers of a single state. This transborder, impact, may happen because the scope of enforcement of domestic policies often encompasses activities taking place beyond territorial borders. Laws from one country can also serve as templates or sources of inspiration from one country to the other.[7]

The overwhelming majority of the stakeholders surveyed expressed that in Latin America foreign regulatory approaches do impact domestic efforts. In numbers, 80.5% indicated that domestic regulatory initiatives are either 'very much' or 'rather much' inspired by foreign ones. 17% of stakeholders stated that they were inspired 'to some extent', and only 2,5% expressed that they were 'only a little' inspired. None of the surveyed stakeholders stated that they were *not* a source of inspiration. In their comments, stakeholders noted that initiatives originating from the US and Europe had more of an effect on the development and application of domestic legal frameworks in LAC countries.

Taken together, the stakeholders have pointed out five reasons for such influence: (i the social and cultural affinity between the US and Europe with LAC legal systems; hence decision-makers are more prompt to seek out such foreign sources as inspiration; (ii the global nature of the internet pushes towards harmonization and looking at approaches outside the region is relevant; (iii international treaty obligations encourage consideration of global solutions; (iv the belief that countries outside the region are more experienced with digital technologies and have a more intimate grasp of the problems they may bring; and (v not all countries have the technical capacity to deploy and implement such regulations; thus international technical cooperation mechanisms

6 The Internet and Jurisdiction Policy Network have prepared three Framing Briefs on user data access, content moderation challenges and abuse at the DNS level in the context of Covid-19, respectively. Please see: https://www.internetjurisdiction.net/publications.

7 Bradford, Anu. The Brussels Effect: How the European Union Rules the World, OUP, 2020..

bring international initiatives and approaches, helping with implementation. Accordingly, the over-arching trend is that LAC's domestic internet governance and regulation initiatives are inspired by foreign approaches.

As one surveyed stakeholder has mentioned:

> *"Fashions and the need to follow patterns happens all the time. Topics such as cybersecurity, personal data, privacy, for example, are highly observed today. [Yet], not everything is always copied from other legislation. There have been bilateral works: Mexico-European Union, Argentina-European Union. The Chilean Net Neutrality Law was a pioneer. The Brazilian Internet Bill of Rights was also a pioneer. Either way, the debate is global."*

1. There is an increased appetite to regulate cyberspace - Proliferation of initiatives

There is currently a general consensus that some regulation is needed for the internet. However, there is a somewhat lack of consensus on the types of complexities regulation can bring. As the Internet & Jurisdiction Global Status Report 2019 mentions, it is not a matter of whether to regulate but rather how and by whom. Globally, there is an increase in forms of regulation that may include international treaties, domestic laws, administrative regulations, judicial decisions, codes of conduct, domestic or international guidelines, declarations, technical standards, conventions, company and community policies and contractual obligations. These initiatives create an intricate patchwork of normative frameworks —not all of them with legal standing, while nonetheless impacting the policy landscape.

Countries in the LAC region have to grapple with this multitude of initiatives - not all of their own making. Among the responses of the stakeholders, three major phenomena can be identified.

The first relates to the compliance challenges that enterprises face when striving to understand the applicable legal framework. Therefore, the first question that needs to be answered is: which national law(s) is(are) applicable to a specific case?

The second is that complex and multilayered regulation may still create legal uncertainty. Even after ascertaining the applicable national law(s), a plethora of legal instruments might make it harder to navigate the country's legal framework, such as laws, decrees, ordinances, judicial decisions and other legal sources.

The third one relates to unintended consequences that regulatory actions might have. Such consequences might happen because the act of balancing different rules and rights does not necessarily have a predetermined outcome. This is the case of requests of electronic evidence from a cloud service provider, as the data may be covered by different laws depending on where it is being stored (see further, in Section IV.B, No.3). It may be also because the application may have infringed some national rules and, in order to sanction the company responsible for the act, the effects of the sanctioning are felt way beyond a country's border. The blocking of the messenger application WhatsApp in Brazil that affected users in Chile and Argentina is one illustration of that (app blocking is further discussed in Section V.B, No. 6).

The profusion of regulations may solve some of the problems yet is itself a source of others. The majority of stakeholders seem to be of the opinion that there should be more coordination and cooperation around internet policy making in the LAC region and that certain topics are more regulated than others.

2. Legislative and judicial inspiration - cross-fertilization or imitation?

The profusion of national regulatory initiatives may hide the extent foreign legislation and judicial decisions spark national and regional debates in the LAC region. Domestic efforts may mimic, imitate, or even copy approaches and rationales brewed overseas. The literature review and the input from the stakeholders surveyed suggest there is a fine line between cross-fertilization and imitation.

This over-arching trend of imitation is underscored by many cases in different areas of internet regulation where an external effort has resulted in domestic or regional initiatives.

- This has been the case of the discussions on net neutrality in the United States: the approach from the Federal Communications Commission (FCC) provided the basis for the debate on the matter all over LAC. [8]
- The European judgment in the Costeja Case – affirming a "right to be forgotten" - has divided experts, countries, and courts in the LAC region (see Section IV.A, No.3 for more findings on this topic).
- The approval and subsequent entry into force of the EU General Data Protection Regulation (GDPR) has moved many countries to either adopt new legislation or embark on a reform of their data protection regime. No less than four laws on data protection were approved after 2016 (the year when GDPR came into force), and countries such as Argentina, Chile, Colombia and Uruguay, have either initiated review or have reformed their data protection legislation. Some countries have also decided to propose a new general data protection legislation such as Barbados, El Salvador, and Jamaica, just to mention a few (see Section IV.C, No 1).

The recent adoption of the new EU Copyright Directive unleashed discussion on platform liability regimes for third-party copyright violations (see Section V.A, No. 7), with impacts already felt in the LAC region.

The consequences of such influence cut both ways, having positive and negative implications for the region. On one side, stakeholders pointed out that they serve as a harmonizing tool. They approximate national initiatives to foreign ones, having a coordinating spillover effect. Interestingly, in the LAC region, these initiatives might circulate intra-region as well, expanding the consonance across the different countries.

Stakeholders nonetheless expressed concern that in some circumstances, foreign solutions are not appropriate to the social, economic and cultural context of the region. One mentioned that even if the solutions are sound, they may not be applied at an optimal level. The institutions in charge may lack resources or authority to carry out the policy objectives they intend to fulfill.

As a final consideration, if the underpinning rationale of the foreign initiative is contentious or invasive, its circulation in the region may have a similar effect, potentially leading to conflict.

8 Retrieved from: https://www.derechosdigitales.org/wp-content/uploads/neutralidad-de-la-red.pdf.

C. Normative plurality and concern over international influence

In many areas of law, domestic legislation is still the main form of regulation. For the internet however, one can hardly say it is the *only* element regulating and guiding online conduct. Other factors such as international agreements, foreign regulatory initiatives (with and without extraterritorial influence), technical and industry specific standards, national and international guidelines, enterprises terms of use and service, community guidelines, architectural decisions (code) weigh significantly on the online environment as well.

As mentioned in the Internet & Jurisdiction Global Status Report 2019, a pyramidal regulatory model[9] with hard regulation issued by the state cannot account for the profusion of normative initiatives and their relative impact. In the LAC region, countries are both drawn towards foreign initiatives and skeptical of them. What cannot be denied is that a plurality of efforts, not only from states or the region itself, influences and governs online conduct.

1. Rules are set for —and by— established large international actors

Interviewed and surveyed stakeholders called attention to the fact that not all initiatives have an equal impact and not all actors have the same standing in the decision-making process. They have highlighted that in many circumstances bigger states and bigger companies have more of a voice and influence in setting rules for the internet than smaller ones.

Normative initiatives seem to suffer from a gravitational force towards bigger actors. The bigger the actor, the stronger the pull to their ambitions. Norms seem to be set to satisfy the interests of larger nations and enterprises and are less adapted to the circumstances of SMEs and enterprises or smaller or less developed countries.

The majority of stakeholders consider this trend a barrier for SMEs and companies, particularly from smaller states, to compete internationally. Some experts mentioned that most of the smaller nations and enterprises do not have the resources nor the human capital necessary to comply with complex sets of regulations.[10]

As for cross-border transactions and international initiatives, despite some recent successes, companies from the region are still substantially affected by the lack of harmonization and coordination of efforts. LAC companies that act transnationally tend to be financed by foreign venture capital or are acquired by more capitalized foreign companies.

This situation is reflected in the survey where 61% of stakeholders strongly agree or agree that cross-border legal challenges on the internet are a barrier for SMEs in the region, with only 10% disagreeing.

2. The role of company norms: the 'constitutional' status of Terms of Service

Companies, particularly platforms, purport to establish their own rules to regulate online behavior. It is already widely acknowledged that the choices in architecture (code) impact and regulate the conduct of actors online and can impact the possibilities of

9 Ost. F, & van de Kerchove. M. (2002). De la pyramide au réseau? Pour une théorie dialectique du droit, Facultés universitaires Saint-Louis Bruxelles.

10 S. HUBBARD, Fake News is a Real Antitrust Problem. CIP Antitrust Chronicle. 2017, 2.

online[11] activity. Without a "like" button, one cannot express his or her satisfaction or lack thereof to some comment, photo or video online. If a message can be forwarded to one person instead of five or twenty, it is a disincentive to spread information (and disinformation).[12] These are just few examples of how code can impact online conduct.

Yet, code is only one dimension where platforms influence behavior. Terms of Service and community guidelines provide a normative basis for internet service providers to act as regulators and to police cyberspace. Depending on the platform, their level of sophistication may lead them to create institutions that resemble those of a State.[13] Facebook very recently instituted a parallel quasi-judicial body called 'Oversight Board' that will function as an appellate body for its content moderation decisions.[14] E-commerce platforms have dispute settlement mechanisms, even for copyright protection.[15] Reddit allows for communities to provide their own set of rules and counsel them to have active moderators and appeal procedures.[16] The list of platforms and their actions that resemble states' institutions is growing.

These above-mentioned initiatives have given rise to Terms of Service that resemble constitutions. Despite being company norms, they appear to be the first line of recourse. If conduct online is found to be offensive or harmful, actions from platforms are expected, and they are based chiefly on their Terms of Service. At the same time, they are increasingly affirming users rights, in an almost 'constitutional' way.

These trends have a series of overarching consequences. The first one (discussed below in Section III.E.) is that platforms are called on to be more responsible for what happens inside their domains. Second, they can act across jurisdictions, since rules of conduct are not bound by states' frontiers. A company can change the terms in all their platforms, across all or selected countries. Third, enterprises can agree amongst themselves on particular common standards and implement them in a coordinated fashion, independent of state coordination.[17]

In another set of implications, these company norms lack a public or democratic approval process and can potentially clash with national regulations. In the LAC region this clash has happened on more than one occasion. The case that has caught international attention has been regarding 'stay-up orders' —judicial decisions that mandate platforms to keep speech online, despite allegedly violating Terms of Service.[18]

These company norms may facilitate cross-border harmonized standards and their transnational application brings international discussion, potentially encouraging a coordinated or harmonized response. Surveyed stakeholders, however, called attention to the lack of transparency and clarity in setting up such terms. In the comments, one stakeholder noted that the global DNA of such Terms of Service —set up by mostly multinational platforms— may not be prepared or flexible enough to encompass the

11 Example retrieved from: 'Like' Button Battle: Facebook Agrees to Voluntary Privacy Code, SPIEGEL ONLINE (Ger.) (Sept. 8, 2011), http://www.spiegel.de/international/germany/0,1518,785190,00.html.

12 This refers to the changes the messenger WhatsApp has made to its architecture diminishing the possibility to resend messages that had already been forwarded too many times. Retrieved from: https://www.theguardian.com/technology/2020/apr/07/whatsapp-to-impose-new-limit-on-forwarding-to-fight-fake-news.

13 Chander, A. Facebookistan. In.: Southern California Law Review, Vol. 86, No. 1, 2012. Retrieved from: http://ssrn.com/abstract=2061300. See as well: Mackinnon, R. Facebookistan and Googledom. In.: Consent of the Networked. Basic Books, 2012.

14 Retrieved from: https://about.fb.com/news/2020/05/welcoming-the-oversight-board/.

15 https://www.mercadolivre.com.br/brandprotection/enforcement

16 Retrieved from: https://www.redditinc.com/policies/moderator-guidelines-for-healthy-communities.

17 This has recently happened through a joint statement against the spread of misinformation in relation to Covid-19 pandemic. Retrieved from: https://techcrunch.com/2020/03/16/facebook-reddit-google-linkedin-microsoft-twitter-and-youtube-issue-joint-statement-on-misinformation/.

18 Waqas, Brazil will sue Facebook for blocking picture of indigenous woman, HackRead (April 20, 2015) https://www.hackread.com/facebook-blocking-brazil-indigenous-picture/. For analysis of stay-up decisions, see: https://cyberlaw.stanford.edu/files/Dolphins-in-the-Net-AG-Analysis.pdf.

diversity and idiosyncrasies present in local realities, particularly in smaller and developing nations as in the LAC region. One could say that there is a risk that the 'constitutions' of global platforms may not be inclusive enough for the local realities of smaller countries.

D. The role of territoriality and the exercise of sovereignty on a global network

The concept of territoriality has been difficult to reconcile with some of the features of cyberspace. Territoriality is supposed to fulfill the function of a guiding principle to both provide grounds for a state to exercise power and to define this power's geographical extent - a topographic limit to a state's sovereignty.

The internet, on the other hand, was developed to be borderless or at least border neutral, so that information can flow despite geographical barriers. Hence, a territorial jurisdiction loses its precise meaning in a cyberspace that was not supposed to mirror the underlying political state divisions of the physical world. Countries cannot, however, deny that certain online actions impact both property and people that are in the physical world, and within their allotted territory. The increased interconnection of physical and virtual worlds blurs the lines between the two, further leading to more geographically extensive state regulations.

States have sought to use the location of persons, devices, or servers as territorial anchor-points to justify the exercise of jurisdiction online. To a certain extent, jurisdiction is ascertained towards legal acts that may be linked to more than one territory and potentially to more than one jurisdiction. The consequence is that in some cases states have either 'overreached' —attaching jurisdiction where there is only a tenuous connection, or 'under-reached'— meaning certain victims are left without recourse.

The LAC region has a unique relationship with the legal concept of territoriality, being considered as the birthplace of the principle of non-intervention.[19] It is not an accident that the most famous definition of 'State' comes from a convention drafted in the region, the Montevideo Convention on the Rights and Duties of States of 1933. It defines territory as one of its constitutive elements.[20] This context has implications for understanding certain subject-matters as being within the purview of the domestic jurisdiction of a state. It is against this background that states in the region conceptualize territorial jurisdiction, even online.

Being the birthplace of the principle of non-intervention colors LAC's understanding of jurisdiction. This approach is illustrated by the treatment of foreign companies that appear not to follow domestic laws. The escalation to blocking or arresting company executives seems to be a consequence of this notion: within its territory, a state's law has to be respected. Similarly, with e-evidence, it appears that national law enforcement agencies are puzzled when they do not have access to data on crimes that happened within their borders.

In some circumstances, the jurisdiction's rationale is both territorially-dependent and territorially-independent. There is an appetite to regulate what happens on or impacts LAC's territory, but once it does, jurisdiction may be thus extended beyond the region. For example, extraterritorial applications of data protection regulations and conditions for cross-border personal data transfers. In cases of defamation and content

19 For an overview of the development of the principle see: Tillman, R. And Scarfi, J.P. Cooperation and Hegemony in US-Latin American Relations, Palgrave Macmillan, 2016. For one of the first statements of the principle, see: Alvarez, A. Latin America and International Law. In. the American Journal of International Law. Vol. 3, No. 2 (Apr., 1909), pp. 269-353.

20 Retrieved from: https://treaties.un.org/doc/Publication/UNTS/LON/Volume%20165/v165.pdf.

moderation, take-down orders on many occasions focus on removing speech or even removing whole accounts with a global and not only local reach.

There is an overarching trend to focus jurisdiction more on the basis of location of behavior or conduct than on the location of where data is stored. Yet, the location and movement of data is still sometimes a relevant factor to be considered.

1. An increasing geographic reach of national laws

States find it increasingly troublesome that the fluidity of the online environment —imposing no clear barriers for cross-border interaction— is exploited so that domestic legislation may be circumvented. Understandably, states want regulation to discourage such behavior. The rationale is that laws should be respected online as much as in the offline world. Each state considers as its right to govern, what happens and what is available online. There is a perception that if it impacts or has an effect on a state's territory, then the behavior has to fall within that state's jurisdiction.

In the absence of international or regional binding instruments, many states, including in the region, end up making broad claims of jurisdiction through either new legislation or expansive interpretation of existing ones. In the LAC region, this overarching trend is particularly visible in the areas of data protection (Section IV.C) and access to electronic evidence by law enforcement agencies (Section IV.B).

In the view of the surveyed stakeholders, this approach to regulation - increasing the geographic reach of national laws - can lead to either arbitrary enforcement or frustration. As for the latter, actual enforcement might be difficult or nearly impossible in certain cases. Regarding the former, people may be surprised by prosecution in a faraway country, without noticing or being aware that they had violated a local law. Another aspect is that the scope can be so broad that it may be challenging to define which behaviors will be encompassed, in which case enforcement may seem discretionary.

A parallel global trend picked up by countries in LAC is to enact regulations with steep fines for non-compliance. Threats of sanctions are used to encourage compliance. The concern shown by LAC states is that with less overwhelming sanctions, their laws will be an afterthought and may be ignored by international players. The difficulty with this rationale seems to be that it motivates other countries to do the same and compete for the highest fines and the harshest sanctions, preventing the flow of data and business.

2. Challenges of enforceability

Broad jurisdictional claims may be difficult to enforce, and the broader they are, the harder it may be. Claiming jurisdiction is not the same as being able to enforce it. A state applying its laws based on a weak link - between conduct and the state itself - may find it difficult for its actions to be seen as legitimate. Similarly, affirming jurisdiction, without the capabilities of enforcing it, may be detrimental to the perception of the efficacy of the regulation. It may run counter to the objective of encouraging compliance.

To lay broad claims of jurisdiction, however, may be a strategy in itself. It makes clear that a specific matter touches an important societal value. In other words, that the state cares for that subject. This strategy may be intended as a form of drawing jurisdictional lines and articulating a point of view on the extent of a states' interests.

A state may also see a need to rely on cooperation with another state. Real assets might be in another country, and data *idem*, hence, out of the enforcer's country reach or not realistically within its grasp. Thus, regulatory clashes may potentially occur, constituting both a challenge to interstate cooperation as much as an opportunity to find mutually acceptable solutions.

This is reinforced by the fact that once jurisdiction is asserted, the country has to be willing to see it reciprocated - an equally broad jurisdiction from other countries. The LAC region has an international tradition of reciprocity. Thus, foreign affirmations of jurisdiction find fertile ground to be duplicated domestically.

Several stakeholders called attention to the fact that countries in LAC might not all have the same capabilities to extend their jurisdiction beyond their borders. They noted the differences in size, economy, and power between the countries in the region and highlighted the potential hurdles they may face to mirror outside action. Hence, an extraterritorial or broad assertion of jurisdiction from a LAC country may be put to the test when needing enforcement.

The opposite direction is true as well. Surveyed stakeholders mentioned that smaller nations might be powerless when bigger nations flex their legal muscles. The case of online gambling brought by Antigua to the WTO represents an illustrative example. Although the dispute was ultimately decided by the appellate board in favor of the US, it would have been challenging for the Caribbean nation to assert its rights and safeguard its businesses against a North-American law with cross-border effect. In actuality, even if legal from the standpoint of the WTO, the outcome ended up being a ‘market destroying measure’, the service could no longer continue.

E. New roles for intermediaries

Intermediaries are very diverse: search engines, social media networks, e-commerce or streaming platforms, digital payment mechanisms, and many other actors that facilitate the most well-known activities online. As the internet developed to be more mainstream, intermediaries have gained in relevance, becoming integrated into the routine of internet users. They have become the conduits that connect different people and businesses and facilitate transactions. The result is a change in the morphology of cyberspace, moving from a somewhat self-organized wilderness, into multiple organized relatively walled gardens.

The degree of dependence on such internet intermediaries disputed. Yet, it is clear they represent a significant part of the traffic and, from a user-centric point of view, they simplify internet use. With this newly achieved centrality a discussion has emerged on the roles and responsibilities of these actors for what happens in cyberspace. Intermediaries are seen as having to share more on the burden of controlling what happens online.

1. Increasing responsibility bestowed on private operators

Traditionally, countries have regarded internet intermediaries as deserving legal protection due to their important function as crossroads, gateways or meeting places for internet users. However, a series of situations involving child pornography, explicit violence, terrorism, divulgation of intimate images (‘revenge porn’), disinformation campaigns (‘fake news’), large scale copyright infringements, among others, have exposed the shortcomings of such approach if taken without precautions.[21]

[21] Retrieved from: Frosio, G. (d). Oxford Handbook of Online Intermediary Liability. OUP, 2020.

Countries in the LAC region share an approach of bestowing a larger role on private operators in internet governance. For countries in the region, the matter has gained relevance particularly in the fields of hateful and harmful speech, disinformation (chiefly in the context of elections), copyright infringements, the sale of counterfeit goods, and privacy and data protection.

Intermediaries end up playing quasi-state functions, for instance, in their quasi-judicial role deciding on taking down content and suspending or removing accounts on repeated copyright offenders. They are the ones called to decide on the legality of content, whether it is political satire (allowed) or defamatory speech (not permitted) for example. They may take such actions voluntarily in accordance with their Terms of Service or mandated by domestic regulation and court decisions.

Legal regimes that until recently shielded intermediaries from prosecution have given rise to more nuanced approaches.[22] In the LAC region strategies have varied among countries. Venezuela and Cuba seem to be among the strictest ones, having enacted legislation that imposes obligations on internet service providers (ISPs) to monitor and 'regulate' speech. Besides, they provide extensive powers for public agencies to even shutdown intermediaries that disrespect their authority.[23] Other countries have sought to regulate specific areas such as hate speech, making intermediaries liable if they don't take down speech considered illegal. Other approaches have been to issue codes of conduct or enter into administrative agreements with intermediaries.

Surveyed stakeholders emphasize that this trend may have cross-border implications. This is particularly acute in cases where companies are left with no choice but to comply with one state's regulation (including a judicial order) and risk violating the legal regime of another if there is a conflict of laws. The consequences might not be easy to foresee, especially for a LAC country. Enterprises may implement a 'most strict common denominator' approach, which may limit freedom of expression in the region, or, when pressed, companies may choose not to implement local laws, which may impact domestic legal legitimacy.

Stakeholders noted as well that requiring platforms to take such a role as internet gatekeepers, may erode the legitimacy of and confidence in state institutions and the sense of justice. In situations involving elections, it may impact the democratic process. Companies become in charge of what information can circulate and how. Yet disinformation may as well have a detrimental effect to the democratic elections. LAC countries, as much as other states around the globe, have to balance the pros and cons of the new roles of internet intermediaries and how risks may be mitigated.

22 As an example, the Brazilian Internet Bill of Rights ('Marco Civil da Internet' - Law N. 12965/2014) enshrines a 'safe harbor' provision. Chilean Law N. 20430/2010 Reformed its copyright legislation to provide a 'safe harbor' provision from third party liability in what concerns internet copyright.

23 Retrieved from: http://www.leyresorte.gob.ve/wp-content/uploads/2012/07/Ley-de-Responsabilidad-Social-en-Radio-Television-y-Medios-Electrónicos.pdf; and Special Rapporteur on from of Expression OAS, Special Report on the Situation of Freedom of Expression in Cuba, 2019. Retrieved from: http://www.oas.org/es/cidh/expresion/docs/informes/Cuba-es.pdf.

IV MAJOR TOPICAL TRENDS IN THE LAC REGION

A. Expression

1. Fake news and disinformation campaigns are triggering countries in the region to seek regulatory action

The internet has lowered barriers for citizens to inform and express themselves. At the same time, disinformation - mass dissemination of information that is either false, out of context or intent in inflicting harm —has also gained in prevalence.

The speed, volume, and "virality" of informational flows challenge the ability to control them. The use of personal data for microtargeting campaigns[24] and the effect some algorithms have of creating filter bubbles[25] or echo chambers - where people see, hear and listen only to what they want or expect —enhances the need for sound access to information. This may also affect people forming their thoughts, ideas, and opinions without undue influence.

This situation is particularly acute during elections. The stakeholders surveyed repeated many of the concerns international actors have conveyed. Disinformation may lead to polarization,[26] information silos, voter suppression,[27] manipulation of the political agenda, among other negative impacts.[28] One stakeholder mentioned that attacks and manipulation come from both foreign and domestic actors using the network to intentionally sow division and polarization.

As one interviewed stakeholder has stated:

> *"Election interference is a major threat to the universal right of people to take part in the democratic process. This is an issue that both governments and technology companies are grappling with to meet the challenges of the latest election meddling tactics and technologies. It is worth noting that attacks and coordinated manipulation are no longer coming from malign foreign powers alone. Increasingly, the interference in election processes is used by domestic actors trying to sow division and polarization in both authoritarian and democratic contexts."*

24 Retrieved from: https://datasociety.net/wp-content/uploads/2018/10/DS_Digital_Influence_Machine.pdf.
25 Retrieved from: Pariser, E. The Filter Bubble: What the Internet Is Hiding from You. New York: Penguin, 2011.
26 Sunstein, C. #Republic: Divided Democracy in the Age of Social Media. Princeton University Press, Princeton, 2017.
27 A. Mcstay. Fake news and the economy of emotions: problems, causes, solutions. In.: Digital Journalism, 2018. Retrieved form: https://www.tandfonline.com/doi/full/10.1080/21670811.2017.1345645.
28 OAS. Guide to guarantee freedom of expression regarding deliberate disinformation in electoral contexts, 2019. Retrieved from: https://www.oas.org/en/iachr/expression/publications/Guia_Desinformacion_VF%20ENG.pdf

LAC countries have responded to these trends in a variety of ways. Most of them have followed a trend to draft regulations either criminalizing the spread of disinformation —usually under the heading of the so-called "fake news"— or imposing a duty for internet platforms to be more proactive in their monitoring of speech, often shifting the liability burden to the internet intermediaries.

The threat of criminalization has been the strategy used in Peru, for instance, where the Ministry of Justice stated that speech that manipulates citizens in order to obtain a benefit or disturb the public order might be criminally punished.[29] Some countries, such as Brazil have started inquiries into how a network of disinformation is financed.[30] This strategy of 'following the money' may shut down the tap that allows disinformation to flow. Other countries, including Argentina, Colombia, Costa Rica, Mexico, and Uruguay, have raised public discussions on the matter in order to steer platforms to integrate fact-checking initiatives in their architecture.[31]

There is little doubt that the fight against disinformation has cross-border impacts: companies offering goods and services across borders will have to adapt policies to deal with these newfound responsibilities.

2. The non-consensual distribution of sexually explicit media knows no border and can perpetuate damages

The non-consensual distribution of sexually explicit media can happen through different forms. It can happen by strangers who intentionally publish sexually explicit media online or by someone who knows the person in the intimate sphere and commits what is commonly called as revenge pornography (or revenge porn).

Countries in the LAC region have been taking different approaches to tackle the issue. In some cases, the distribution of non-consensual sexually explicit media could be treated as defamation cases, while other legislation provide for a specific approach, altering their criminal legislation to treat the practice as a new criminal conduct.

In Uruguay, non-consensual distribution of sexually explicit media is a crime, and internet platforms are subject to sanctions if they do not immediately take the content down.[32] Other countries are discussing bills to specifically address the non-consensual distribution of sexually explicit media, such as Chile[33] and Peru.[34]

29 Peru, Gestión, Personas que difundan noticias falsas podrían recibir hasta 6 años de prisón (2020, April 08). Retrieved from: https://gestion.pe/peru/coronavirus-peru-personas-que-difundan-noticias-falsas-podrian-recibir-hasta-6-anos-de-prision-segun-minjus-ministerio-de-jusiticia-estado-de-emergencia-cuarentena-nndc-noticia/?ref=gesr.

30 Brazil. Supreme Court (STF). Inquiry 4781. Retrieved from http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=444198&ori=1.

31 The public fact-finding platform 'Confiar' from Argentina is an example of that. Retrieved from https://www.argentina.gob.ar/noticias/confiar-la-plataforma-oficial-para-combatir-la-infodemia. Also, fact checker organization Chequeado, created in Argentina, has coordinated the LatamChequea coalition with 35 organizations from Latin America. See more at: https://chequeado.com/latamcoronavirus/.

32 Uruguay, Ley nº 19580/2018, Article 92. Retrieved from https://www.impo.com.uy/bases/leyes/19580-2017.

33 Chile, Boletíns nº 11923-25 and 12164-07. Retrieved from https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=12444&prmBoletin=11923-25.

34 Peru, Law projects 01669/2016-CR and 2460/2019, both foreseeing criminal responsibilities to perpetrators. Retrieved from http://www.leyes.congreso.gob.pe/Documentos/2016_2021/Proyectos_de_Ley_y_de_Resoluciones_Legislativas/PL0166920170717.pdf and http://www.congreso.gob.pe/comisiones2016/Justicia/ProyectosLey/.

The difficulty in enforcing such content removal, sometimes due to jurisdictional issues, can also bring life-altering consequences to women. In Colombia for instance, the sender of threats against a woman could not be identified because they were sent from a public place (an internet café). In another case, the perpetrator could not be identified because the address was a location in the United States.[35]

3. The Google Spain case at the ECJ has sparked a regional debate about the "right to be forgotten"

The decision of the Court of Justice of the European Union on the 2014 Google Spain[36] case has unleashed a region-wide discussion. The debates address the legal orders of many countries who have already recognized a so-called "right to be forgotten" and whether it is prudent or even desirable to institute such a right. Such discussion is more appropriately understood as a right to request "de-listing" or "de-indexing". Because the judgment does not establish such a requirement, the content itself is not erased. Instead, search engines such as Google, Bing and others are only urged to suppress the results of queries based on the individual's name - and other personal identifiable markers - connected to the information that is deemed irrelevant, outdated, or without actual value.

The Google Spain case has motivated a series of claims affirming such a right in the context of the region. Differences in data protection regulations (or lack thereof) have not impeded some domestic courts to acknowledge the existence of "a right to be forgotten" and to order search engines - and sometimes news outlets themselves - to de-list information.[37] More often than not, the parameters of this right were left unclear: its scope and even who should be responsible for de-listing and under which conditions are left open.[38]

Other courts have dismissed the right or qualified it.[39] The history of protecting freedom of expression in the region tends to act as a counter-weight to de-listing, particularly without a court order.[40]

4. Stakeholders recognize the global scope of the right to be forgotten

Surveyed stakeholders were asked whether the right to be forgotten had attained global status or was applicable to the LAC region as a whole. One of the stakeholders mentioned that the expression "right to be forgotten" has been used in LAC as an all-encompassing term, including every instance where users demand ISPs to remove, de-index, de-list or hide content. Others thought that the concept behind the right is

35 Case Study Number 1, Colombia, from the Association for Progressive Communications (APC)'s research End violence: Women's rights and safety online. From impunity to justice: Domestic legal remedies for cases of technology-related violence against women (p. 12). Retrieved from: https://www.genderit.org/sites/default/files/flow_domestic_legal_remedies_0.pdf.

36 CJEU, Case C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 2014.

37 Retrieved from: https://law.stanford.edu/wp-content/uploads/2017/09/The-_Right-to-Be-Forgotten_-and-Blocking-Orders-under-the-American-Convention-Emerging-Issues-in-Intermediary-Liability-and-Human-Rights_Sep17-.pdf.

38 Retrieved from: https://www.palermo.edu/cele/pdf/investigaciones/Towards_an_Internet_Free_of_Censorship_II_10-03_FINAL.pdf.

39 One of the most important cases involved the question whether intermediaries could be held liable for content which impact on privacy or reputation. The court understood that de-listing should only apply with a court order and or with unlawful information. (Argentina, Supreme Court, Case "Rodríguez M. Belen c/Google y Otro s/ daños y perjuicios," Judgment R.522.XLIX, 10/28/14.) In Brazil, the right has received extensive debate and was subject of a public hearing at the Brazilian Supreme Court STF. The Superior Court had granted the right under qualifications. Minutes of the debate on the Aida Curi Case are available here: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/AUDINCIAPBLICASOBREODIREITOAOESQUECIMENTO_Transcries.pdf.

40 Retrieved from: https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2016/04/GFOE-Presentation-Catalina-Botero-.pdf.

gaining momentum and that certain courts and countries were recognizing it. 70,73% of the surveyed and interviewed stakeholders agree or strongly agree that the right to be forgotten is indeed a global concept.

> As one surveyed stakeholder remarks: "The right to be forgotten is a new right proposed in the context of information society. Reactions to this right vary from country to country because the concept and rationale are not yet clearly defined. The absence of consensus on this point has the potential to create uncertainty in a society that is becoming increasingly borderless. Country-specific decisions are not enough for the smooth development of this concept, and there is an urgent need to reach a consensus around core points. Given the borderless character of today's world, the conflict between fundamental values, protecting the dignity of an individual versus the right to know and to guarantee freedom of expression, comes with varying results."

5. Regional experience with amnesty laws and a right to remember created a backlash to the enforcement of a general right to be forgotten

Certain elements of the legal order, history and culture of the region diverge from its original European roots. For instance, many countries of the LAC region have passed through very recent authoritarian regimes, when several of their leaders have been accused of egregious human rights violations. Most of the states, while transitioning to democracy, have issued amnesty laws, pardoning those responsible for the human rights violations and in many cases blocking both access to the truth regarding what has happened, as well as any sort of reparation.

Under the substantial guidance of the Inter-American Human Rights System,[41] in the last few decades, there has been an effort to develop the opposite right, a "right to remember", a right of the victims to have access to the truth. Under such right, amnesty laws were repelled, "Truth Commissions" were established, and even perpetrators have been prosecuted.

Data protection experts, authorities, and civil society organizations,[42] now understand a "right to be forgotten" as running contrary to such cultural and human rights tradition.[43] Hence, regionally, de-listing as a concept has to exist alongside a "right to remember", particularly in situations concerning information on alleged or actual human rights violations.

41 The views of the the Inter-American Human Rights System can be seen at the Report "Standards for a Free, Open and Inclusive Internet", 2016, paras. 134 ff. Retrieved from: http://www.oas.org/en/iachr/expression/docs/publications/INTERNET_2016_ENG.pdf.

42 R3D Report "El erroneamente llamado "derecho al olvido" nos es un derecho, es una forma de censura", 2015. Retrieved from: https://r3d.mx/2016/07/12/el-erroneamente-llamado-derecho-al-olvido- no-es-un-derecho-es-una-forma-de-censura/; Hiperdrechos Report "Protección de datos personales: la nueva puerta falsa de la censura", 2016. Retrieved from: http://www.hiperderecho.org/2016/07/proteccion-datos-personales-la-nueva-puerta-falsa-la-censura/.

43 There are those that considered it "an insult" to the history of the region. Eduardo Bertoni. The Right to Be Forgotten: An Insult to Latin American History, 2014. Retrieved from: https://www.huffpost.com/entry/the-right-to-be-forgotten_b_5870664. Another general analysis from the former OAS Special Rapporteur for Freedom of Expression, Catalina Botero can be found at: Retrieved from: https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2016/04/GFOE-Presentation-Catalina-Botero-.pdf.

6. Defamation cases are triggering debates about cross-border effects of the defense of someone's honor and reputation

The respect and protection of personal honor and reputation are found in the laws of a multitude of countries with diverse cultural backgrounds. As a core common understanding, defamation is illegal both offline and online. Implementation, interpretation, and extension of such concepts, however, vary considerably. The internet has exacerbated the importance of such legal differences and has provided more chances for conflict amongst the jurisdictions.

Cross-border issues arise particularly under three areas: (i speech published overseas and impacting domestically; (ii the medium employed for publication is outside the country where the person offended has its habitual residency or work - either because the company providing the service is established in another country or because the servers are; and or (iii the damage to honor or reputation happens in more than one jurisdiction.

The Internet & Jurisdiction Global Status Report 2019 called attention to the fact that this is not novel. Due to the potential global geographical reach of the internet, cross-border issues of defamation have been a common occurrence online. This issue may have further cross-border implications. For example, in the LAC region, requests for damages in defamation cases have often been accompanied with requests for removal of the content deemed defamatory or for rectification. Plaintiffs frequently pursue internet intermediaries that are put in the situation of complying with judicial orders and having to decide the territorial scope of such orders.

That was the case of Google with the service "blogger.com". Colombian[44] and Mexican[45] courts have requested that Google remove blog posts from individuals that were considered defamatory. In Brazil, it was Facebook that was ordered to remove content and take down a whole profile deemed to be defaming a political candidate.[46] Each of these cases contributes to an understanding that such content would not be available worldwide.

7. Defamation is both a civil and a criminal offense in many countries in the region, raising additional questions about how the protection of honor might restrict freedom of expression (e.g. for journalists and bloggers)

In many countries in the LAC region, defamation is not only a civil matter, but also a criminal one.[47] The criminalization of speech that violates the right of honor is still a widespread legal tradition in the region, despite the efforts of the Inter-American Human Rights System condemning it as an undue restriction to freedom of expression. Online defamation may also have criminal repercussions, which may be even more worrisome concerning speech during elections when the suggested remedy should be preferably rectification or the right to a response.[48]

44 Colombian Constitutional Court rules that Google must delete a blogger.com blog that contained defamatory statements. I&J Retrospect Database. Retrieved from https://www.internetjurisdiction.net/publications/ retrospect#article-6369_2017-10.

45 Internet & Jurisdiction Policy Network. (2017, December). Mexican Supreme Court rejects Google's argument that Mexican courts do not have jurisdiction over the platform. I&J Retrospect Database. Retrieved from https://www.internetjurisdiction.net/publications/retrospect#eyJ0byI6IjIwMjAtMDMifQ==.

46 Retrieved from: https://olhardigital.com.br/noticia/juiz-manda-bloquear-facebook-em-todo-o-brasil-por-24-horas/62909.

47 As an example see the overall study conducted by the Committee to Protect Journalists on South American criminal defamation laws: https://cpj.org/reports/2016/03/south-america.php; and one from the International Press Institute on Criminal Defamation laws in the Caribbean: https://ipi.media/ipi-adds-caribbean-defamation-laws-to-online-database/.

48 Retrieved from: https://www.oas.org/en/iachr/expression/publications/Guia_Desinformacion_VF%20ENG.pdf.

The criminalization of speech that violates honor also has a chilling effect on the activities of professional journalists, "citizen journalists" and bloggers alike, especially in small towns of the LAC region. Authorities might severely hinder their speech when their own liberty might be at stake when breaking the news and producing reports that might not please local authorities.

B. Security

1. There is a growing need for coordination in cybersecurity to overcome widespread incidents in the region

The growing level of interconnectedness between off and online worlds —particularly with the so-called Internet of Things— makes issues of security even more important. The LAC region has become an increased *locus* of cybersecurity incidents. At the same time, it has become a major harbor for launching such actions. Coupled with that is the fact that many of the most popular internet services used in the region tend to be foreign, and significant amounts of data pass through or is stored outside the LAC region, chiefly in more developed countries. This generates cross-border challenges that extend from difficulties determining the location of cybercrime to access to evidence, control over the standards of data security, and issues regarding surveillance.

One surveyed stakeholder remarked on the tension of expedite access to data and resolution of cybersecurity incidents with respect to national legal identities and jurisdictional sovereignty. High numbers of stakeholders noted international cooperation on such cross-border issues is paramount to facing this challenge.

2. Cross-border cases of corruption in the LAC region has fostered a sophisticated debate over practices of multi-jurisdictional investigations

Corruption is not a feature for which the LAC region is proud to be known for. In the last two decades, scandals have escalated from isolated cases involving chiefly domestic matters to organized schemes, some encompassing more than one or even several jurisdictions. A significant example has been "Operation Car Wash" ("*Operação Lava-Jato*") that started as an investigation in Brazil but uncovered sophisticated arrangements across dozens of countries. The company Odebrecht, for instance, has been the focus of investigations in several states in the region, former presidents or vice-presidents of at least five countries are in prison or investigated. Several high-level politicians from other countries are also under investigation.[49]

These multi-jurisdiction corruption schemes lead to investigations that have demanded cross-border cooperation of law enforcement agents and several other agents, with important jurisdictional debates. Perhaps the most salient of them is access to digital evidence in multiple jurisdictions and the need to reform the international cooperation instruments that provide both mechanisms for preservation of and access to electronic evidence across borders.

49 An overview of the corruption scandal: https://www.bbc.com/news/world-latin-america-41109132.

3. Access to digital evidence in multiple jurisdictions triggers a review of known practices of investigations in the LAC region

In the course of a multi-jurisdiction investigation, domestic law enforcement agencies need to have access to information that may be located in another country. This may be due to the actions occurring across jurisdictions. For example, a company could wire funds to an off-shore account of a corrupt official; or alleged criminals use internet services that store data overseas run by services through the cloud. Evidence produced in one investigation can be relevant for another and in some cases, investigations on a foreign corruption case impact the security of an investigation in another country.[50]

The fact that relevant data may have a connection to other countries creates a series of jurisdictional issues. It is important to note, however, that there is a distinction between jurisdiction over the crime itself and jurisdiction over evidence necessary for investigation of this very crime.

As for jurisdiction over evidence, there are still multiple issues in discussion. Firstly, there may be a dispute about the connection factor necessary to ascertain jurisdiction over digital evidence. The most common connecting element has traditionally been the location of the evidence. It brings at least two difficulties with it. Due to its digital nature and potential fluidity, digital evidence (data) can be split amongst different jurisdictions or be transferred to another location without warning or effort. Cloud services do both those actions, divide packs of information, and move them constantly across servers, which may and usually are in different jurisdictions.

The location of the data is not the only possible connection factor. There may be others, such as nationality, domicile, or habitual residency of the data subject, or the place of establishment for the company in possession of the data.

Additionally, a request to have access to foreign stored data may be dependent upon cooperation with the country where the data is located. Traditionally as well, foreign and domestic requests are subject to different criteria and procedures. Hence, the validity and enforceability of a foreign request to produce evidence may be disputed.

Finally, countries may impose blocking statues that do not allow international communication of data unless under specific circumstances and procedures. Some data protection legislation, for example, do block transfers without a domestic warrant or consent, for instance.

Surveyed stakeholders highlighted the relevance of access to evidence stored overseas for criminal investigations and the need for cooperation and exchange of information. They noted as well that international processes may be cumbersome and may not be adapted to the exigencies of urgency and speed of the current times, thus suggesting a change in the paradigm for the region.

4. Regional stakeholders do not advocate for the overhaul of the mutual legal assistance system and instead support its adaptation to the digital age

The traditional way to request extraterritorial evidence is through international cooperation. There is a net of international agreements that provide legal procedures to facilitate cross-border assistance and cooperation.

50 For an analysis of the interconnectedness of corruption, foreign bribery and access to information and evidence, see: http://www.oecd.org/daf/anti-bribery/TypologyMLA2012.pdf.

By far the most common are the Mutual Legal Assistance Treaties (MLATs). States in the region are parties to several bilateral MLA agreements and multilateral ones —universal or regional in reach. The Inter-American Convention on Mutual Assistance in Criminal Matters (1992), for instance, has 26 LAC countries as members.[51] Other specific conventions refer to mutual legal assistance and the need for international cooperation on such matters. In this regard, Article XIV of the Inter-American Convention against Corruption (1996) has virtually all countries in the region beside Cuba as parties.[52]

The MLA treaty system is a step up from the traditional use of diplomatic cooperation and rogatory letters, yet it has its own set of difficulties. These challenges are dependent upon countries being parties to MLATs, and procedures are not uniform, as they may change from agreement to agreement.[53] Additionally, the administrative system in place was structured to work with foreign requests constituting exceptions. It was not made for dealing with high volumes. The lack of automation and scalability means that such procedures may not be timely. Meanwhile, investigations may stall, potential culprits may not be found, and or remain free, there may even be follow-on crimes, and the evidence may be moved (to another jurisdiction) or destroyed.

Several countries in the region believe that the MLA system requires reform.[54] The majority of the stakeholders surveyed are as well in agreement that there is a need for incorporating more agile procedures in international cooperation arrangements. Some have cautioned, however, that the procedures should respect due process, data privacy, and human rights in general. One stakeholder highlighted the need to guarantee the authenticity of documents and the credibility of the actors issuing the request.

Generally, stakeholders do not advocate for the overhaul of the MLA system, but instead, call for an adaptation to the digital age. They see that most of the issues derive from the fact that internet companies are established overseas with a domestic presence. Their suggestions tend to revolve around a mechanism of direct requests to such companies (as data holders).

There is little consensus however around the instrument to be used for such reform. MLATs being either bilateral or multilateral tend to take time to negotiate and may not encompass all the needs of access to and preservation of information. Meanwhile, countries are seeking out solutions either unilaterally or within like-minded groups.

5. Regional experts agree that the Budapest Convention is a step in the right direction to facilitate cross-border investigations, but it does not solve the problems of MLA system

Several states in the LAC region are parties or have acceded to the Council of Europe's Convention on Cybercrime of 2001 ("Budapest Convention") that amongst other stipulations, establishes mechanisms for international cooperation on cybercriminal matters.[55] Argentina, Chile, Colombia, Costa Rica, Dominican Republic, Guatemala, Mexico, Panama, Paraguay, Peru are parties to the Convention and Brazil was recently invited to accede to it in December.[56] The Convention provides more expedite arrangements so that evidence may be preserved and accessed.

51 Retrieved from: https://www.oas.org/juridico/english/treaties/a-55.html. The convention has a protocol with far less countries parties: http://www.oas.org/juridico/english/treaties/a-59.html.
52 Retrieved from: http://www.oas.org/en/sla/dil/inter_american_treaties_B-58_against_Corruption.asp.
53 Retrieved from: https://www.justice.gov/archives/jm/criminal-resource-manual-276-treaty-requests.
54 Information submitted by States from the LAC to the UNODC. Retrieved from: https://undocs.org/A/74/130.
55 Retrieved from: https://www.coe.int/en/web/cybercrime/the-budapest-convention.
56 Council of Europe, "Budapest Convention: Brazil invited to accede", 2019, available at https://www.coe.int/en/web/cybercrime/-/budapest-convention-brazil-invited-to-accede.

Interviewed and surveyed stakeholders are of the opinion that the Budapest Convention does not solve the problems regarding the MLA system, yet it is a step in the right direction. One of the stakeholders noted that participation in the Budapest Convention provides an important forum of discussion of the hurdles of access to digital evidence.

The members of the convention are discussing an additional protocol[57] that will provide more specific tools to keep up with the pace of time, especially for subscriber data stored in cloud services, for a more comprehensive and expedited regime.[58] One of the significant difficulties, however, is to establish a common baseline of understanding with respect to privacy and other human rights. Some of the surveyed stakeholders expressed such concern.

6. Law enforcement agents in the region are increasingly seeking access to data outside the MLAT structure

As international processes have not yet reached full maturity, several countries have embarked on unilateral initiatives that have consisted of national legal reforms. One of the leading solutions has been to provide legal authority to require direct access to data from those in possession of it, particularly internet service providers.

The United States, has passed the CLOUD Act, which provides a mechanism for law enforcement agencies from countries having a dedicated bilateral agreement with the U.S. to request companies directly to produce the data. It clarifies that the jurisdiction over digital evidence rests on nationality or residency of the data subject (customer of the ISP). Department of Justice guidelines state that domestic internet service providers can be requested to produce data they hold regardless of its location.[59]

Similarly, the European Union has started a project called e-Evidence. It consists of a draft Regulation that creates orders for preservation and access to digital evidence to be sent directly to internet services providing services to the Union, despite the extraterritorial location of the data.[60]

Both projects recognize that there is still a need for international cooperation. ISPs may however be subject to laws in third countries that may prevent them from producing the evidence, thus needing particular procedures to guarantee access to it.

In the LAC region, a few initiatives are addressing the matter. Countries understand that being a party to the Budapest Convention (2001) is a way forward, yet it cannot solve all issues. That situation is triggering a growing effort from law enforcement agents to access data outside the MLAT framework, fostering the adoption of unilateral solutions.

57 Retrieved from: https://www.coe.int/en/web/cybercrime/t-cy-drafting-group.

58 Members of the LAC have mentioned in a UNODC survey the need to update the Budapest Convention as one instance of possible solution. Retrieved from: https://undocs.org/A/74/130.

59 Retrieved from: https://www.justice.gov/opa/press-release/file/1153446/download.

60 Retrieved from: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en. More direct info: European Commission. (2018, April 17). Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters. COM(2018) 225 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/ TXT/HTML/?uri=CELEX:52018PC0225&from=EN; European Commission. (2018, April 17). Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings. COM(2018) 226 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0226&from=EN.

In Brazil, the Supreme Court was called upon to discuss the constitutionality of the MLAT between Brazil and the United States.[61] The discussion hinges on whether a domestic subsidiary of an internet service provider can be called upon to produce evidence held by the parent company located out of the country; and whether article 11 of the Brazilian Internet Bill of Rights ("Marco Civil da Internet") —which indicates that Brazilian law applies to data collected in Brazil or from a device in Brazil— establishes a procedure of direct request of data stored overseas, bypassing the MLAT.

7. Stakeholders reaffirm that "backdoors" would undermine trust in encrypted systems

Surveyed stakeholders have sent out a clear message against the insertion of backdoors in encrypted systems. When asked if that feature would undermine legitimate security interests of users, 82,93% of the stakeholders agree that it does.

This finding is important since law enforcement agents in countries in the LAC region are pushing for a way to decrypt the contents of the messages that are sent through instant-messaging apps. As applications such as WhatsApp become increasingly popular in the region, the pressure to curb end-to-end encryption increases, allowing some form of accessing the contents of the message for criminal investigations.

It is relevant to mention that encryption is a key factor for trust not only in messaging apps, but also for e-commerce, internet banking and all sort of online activities. At the same time, there are other forms of accessing the contents of a message in a dully-authorized investigation —even in end-to-end encrypted instant-messaging apps— that would not hurt the integrity of encrypted systems. That would be the case of having access to the actual device used for communication (like a cellphone) and infiltration of law enforcement agents in messaging groups. Law enforcements agents in the region are exploring such alternatives as the legal debate over the encryption matures.[62]

C. Economy

1. Inspired by GDPR, countries in the LAC region are creating or improving their national data protection regulations

Data privacy (or data protection) has gained momentum in the last half a decade in the LAC region. Some factors weigh heavily into it. The most notable one is the impact of the EU legislation —the General Data Protection Regulation (GDPR)— has had in the transnational legal order. It has sparked in many countries the need to either review data protection legislation or to create one of its own. Potential access (or lack

61 Brazil. Supreme Court (STF), "Ação Direta de Constitucionalidade" N. 51. Retrieved from: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5320379.

62 See https://carnegieendowment.org/2019/05/30/encryption-debate-in-brazil-pub-79219.

thereof) to the European data market is of importance for many countries and the EU is understood as a regulatory model for domestic efforts (this overarching trend was highlighted in Section III.B).

Additionally, the digitalization of many different aspects of society, including public services, and the data breaches that came in addition, have sparked a higher sense of awareness in the population. People know that their personal data is being collected and might become be available for everyone to see if there is a breach.

2. Half of the countries in the region have a specific data protection regulation

Today, 16 countries have a specific data protection regulation (Antigua and Barbuda Argentina, The Bahamas, Brazil, Chile, Colombia, Costa Rica, Dominican Republic, Mexico, Nicaragua, Panama, Peru, Saint Kitts and Nevis, Saint Lucia, Trinidad and Tobago, Uruguay). 7 countries are discussing a bill: Barbados, Ecuador, El Salvador, Guatemala, Honduras, Jamaica, Paraguay. 10 countries do not have a specific data protection regulation: Belize, Bolivia, Cuba, Dominica, Grenada, Guyana, Haiti, Saint Vincent and the Grenadines, Suriname, Venezuela.

Out of the 10 countries that do not have a general data protection regulation, however, the majority have taken steps towards protecting personal data at some level. Dominica, Grenada and Saint Vincent and The Grenadines are parties of the Organization of Eastern Caribbean States ("OECS"), which under its E-Government for Regional Integration Project has approved a Data Protection draft bill.[63] Belize, Guyana, Haiti, and Suriname as members of CARICOM have also taken part in initiatives that relate to data protection: through the Harmonization of ICT Policies, Legislation and Regulatory Procedures' (HIPCAR) there are a series of data protection policies that serve as regulatory guidelines.[64]

3. There is room for improvement and coordination to foster a truly regional framework for data protection

Interviewed stakeholders emphasized the disparity in the region in terms of institutions regarding the protection of personal data. One surveyed stakeholder called attention to the fact that there is a need for regional coordination, to establish common standards of personal data protection that are truly regional.

Some countries in the region, such as Argentina[65] (2000), Uruguay[66] (2008), and Mexico (2010), have established data protection laws in the last decade. Others, such as Brazil (2018) and Panamá[67] (2019) have concluded the process in previous years, drawing clear inspiration from EU's GDPR.

As regional initiatives have been addressing privacy and data protection as a major topic to promote economic integration and growth, it is expected that new efforts will develop to foster regional dialogue on data protection. Dialogues plan to connect the

63 Organisation of Eastern Caribbean States (OECS), Data Protection Act, 2016. Available at https://www.oecs.org/en/procurement/e-gov/data-protection-act.
64 Retrieved from: https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPCAR/Pages/default.aspx.
65 https://www.oas.org/juridico/PDFs/arg_ley25326.pdf.
66 https://www.impo.com.uy/bases/leyes/18331-2008.
67 ttps://www.sucrelaw.com/blog/media/2019/04/Ley-81-de-2019_Sobre-Proteccion-de-Datos.pdf.

experiences of countries whose laws have already been recognized as adequate under the EU standards (as such as Argentina and Uruguay) with countries that are about to face the challenges of implementing a new data protection regulation.

4. Regional initiatives are fostering standardization of cross-border data transfers

At the international and regional levels, there are no general agreements that either provide for the free flow of data or prevent to hinder it. Yet, some regional organizations have launched guiding principles that aim to harmonize different countries' standards.

The Organization of American States, in its principle 11 on "Trans-border Flow of Data and Accountability" acknowledges the need for harmonization on data protection standards in order not to hinder the flow of data across borders.[68]

The standards of protection approved by the Ibero-American Network for Data Protection, which several of the countries in the region are parties of, also contains a recommendation that cross-border data transfers should occur based on a series of requirements that follow similar patterns as the European legislation. For instance, the standards request either countries to be considered adequate or parties wishing to transfer overseas to follow pre-arranged procedures.[69]

5. There is a demand for the creation of a Digital Single Market in the region

Most of the states in the LAC region are parties to one or more regional organizations and agreements involving transnational digital trade, such as the OAS, ECLAC, CAN, CARICOM, ALADI, APEC, SICA, MERCOSUR, TLCAN, Mesoamerica Project, Pacific Alliance and the TPP.[70]

However, there is still much to be developed in the region in what concerns common infrastructure and harmonized legal frameworks. A unifying central entity with the capacity to bind countries to their initiatives is not present. Enforcement efforts as well are left for each jurisdiction to manage separately.

Stakeholders interviewed mentioned that the difficulties in establishing a Digital Single Market in the LAC region rest on the fact that none of the proposed integration efforts have been implemented successfully. Therefore, jurisdictional differences impact market access and growth opportunities in the region. One stakeholder mentioned that the legal and economic disparity and the lack of minimum common regulatory standards are the most important barriers.

6. Stakeholders indicated that areas such as consumer and data protection, digital payments and tax regimes are key for the creation of a Digital Single Market in the region

Several of the surveyed stakeholders mentioned the digitalization of the economy as an opportunity but underscored a need for regulatory harmonization. Harmonization

68 Retrieved from: http://scm.oas.org/pdfs/2016/CP35451EREPORTCJI.pdf.

69 Retrieved from: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf.

70 ECLAC, Digital Single Market, 2018. Retrieved from: https://repositorio.cepal.org/bitstream/handle/11362/43633/1/S1800569_en.pdf.

was viewed as particularly crucial across areas such as consumer protection, personal data protection, digital identity, digital payments, digital securities, transportation and logistics standards, and taxation regimes.

That perception seems to be in tune with the recommendations of international organizations.[71] There are a few legislative or regulatory initiatives in the region that take into consideration the cross-border challenges of creating a more integrated digital market.[72] When they do exist, they still tend to be conceived from a domestic standpoint, resulting in a considerably fragmented scenario with a multiplicity of standards.

7. The region features a strong consumer rights culture, providing relevant opportunities for the creation of a Digital Single Market

Virtually all countries in the region have consumer protection legislation in force. With just a few exceptions, the majority of countries address consumer protection in dedicated legislation.[73] Some countries do have specific laws on online consumer transactions, yet the majority apply the bulk of the state's consumer protection regime to deal with mostly offline relations. This scenario creates an opportunity for developing a Digital Single Market related to internet platforms and e-commerce as a whole.

The internationalization of the market brings jurisdictional challenges to companies that operate across borders. These companies —including e-commerce, marketplaces and even social media - have to be prepared to comply with consumer protection laws from all the jurisdictions where they conduct business. National consumer protection laws are applicable despite an internet company's place of establishment. The mere fact that they are offering services and goods to a local consumer already triggers national protections.[74]

The presence of a common consumer protection culture in the LAC region has so far co-existed with the lack of a proper harmonized framework or a Digital Single Market, exposing companies to a variety of different domestic standards of protection. Additionally, consumers may seek to resolve their disputes in their own country, resulting in companies being called to appear in courts in several jurisdictions or to take part in different dispute settlement procedures outside their place of establishment.

The lack of common consumer protection standards impact the way internet service providers can interact with consumers in the region. Different consumer protection laws may mean a variety of standards for advertising, unfair billing practices, contract termination, and switching companies (portability and interoperability as well).[75] This situation could pose a barrier to trade.[76]

In MERCOSUR (the Southern Common Market) there are initiatives to harmonize consumer protection standards. Recently, the members proposed to structure and

[71] See for instance study of the OECD: https://www.oecd-ilibrary.org/docserver/9789264251823-16-en.pdf?expires=1588103565&id=id&accname=guest&checksum=233F2DB69A0B854F11BC076348793B73.

[72] CAF, Building a Digital Single Market Strategy for Latin America. Retrieved from: https://scioteca.caf.com/handle/123456789/980?show=full.

[73] ECLAC, Digital Single Market, 2018. Retrieved from: https://repositorio.cepal.org/bitstream/handle/11362/43633/1/S1800569_en.pdf. See as well World Consumer Protection Map: https://unctadwcpm.org. For an overview of several national regimes and how they fair in comparison with other countries in the world, see: MICKLITZ, Hans-W. Micklitz and SAUMIE, Geneviève. Enforcement and Effectiveness of Consumer Law. Springer, 2018.

[74] CAF, Building a Digital Single Market Strategy for Latin America. Retrieved from: https://scioteca.caf.com/handle/123456789/980?show=full.

[75] https://www.oecd-ilibrary.org/docserver/9789264251823-16-en.pdf?expires=1588103565&id=id&accname=guest&checksum=233F2DB69A0B854F11BC076348793B73.

[76] Durovic, M. International Consumer Law: What Is It All About?. In.: J Consum Policy 43, 2020. Retrieved from: https://doi.org/10.1007/s10603-019-09438-9. .

use a digital platform for the settlement of consumer disputes.[77] This could help to foster cross-border internet services and e-commerce in the region, as it diminishes the costs of consumer dispute and litigation.

8. Choice of law and choice of forum clauses tend to be frowned upon in e-commerce due to national consumer protection

To provide more predictability, most internet companies choose to include in their contracts a choice of forum or a method of dispute resolution (arbitration, mediation or conciliation) as well as choice of law clauses. By having these stipulations, they limit the risks of their exposure and simplify the potential jurisdictional entanglement.

Legal regimes worldwide tend to permit such choices under what is called party-autonomy. LAC countries have battled with the concept for the most of the 20th century.[78] It has culminated in the approval of the Mexico Convention of 1994 on the law applicable to international contracts, which, due in part for having enshrined the principle of party-autonomy, has not received wide acceptance: only Venezuela and Mexico are parties to it.[79] In the last two decades, however, the principle has gained traction, and many countries have a more flexible stance, welcoming party-autonomy to certain categories of contracts.[80]

The strong culture of consumer protection has left its mark on the way contracts are interpreted in the region. Many LAC countries understand that contracts where there is an inherent imbalance between the parties - and the stronger party imposes contractual obligations —ought to be the subject of higher scrutiny.[81] The consequence is that choice of law and choice of forum clauses tend to be frowned upon when they may be disadvantageous to the weaker party.[82] In some circumstances, they are seen as abusive, particularly if they limit the means to settle disputes or access to the judiciary. The case becomes even clearer for transactions involving a consumer.[83]

Not only consumer protection laws may apply, but also the choice of forum and law may be considered non-enforceable, particularly if consumers question them in courts.[84]

77 https://www.cancilleria.gob.ar/es/actualidad/noticias/comunicado-conjunto-de-los-presidentes-de-los-estados-partes-del-mercosur.

78 http://www.oas.org/es/sla/ddi/docs/publicaciones_Contratos_Internacionales_OEA-ASADIP_2016_Publicacion_Completa.pdf.

79 Retrieved from: https://www.oas.org/juridico/english/sigs/b-56.html.

80 In the region only Uruguay expressibly rejects party-autonomy - there is some acceptance in the doctrine and case law. In Brazil there is still discussion on its full applicability, the case law is not coherent on the matter. For an overview see Inter-American Juridical Committee Guide on the Law Applicable to International Commercial Contracts, February, 2019. Retrieved from: https://www.oas.org/en/sla/iajc/docs/Guide_Law_Applicable_to_International_Commercial_Contracts_in_the_Americas.pdf.

81 Retrieved from: http://www.oas.org/es/sla/ddi/docs/publicaciones_Contratos_Internacionales_OEA-ASADIP_2016_Publicacion_Completa.pdf.

82 The International Law Association has acknowledged that consumers tend to be the weaker parties in cross-border contracts. See ILA RESOLUTION No.1/2016 Committee on the International Protection of Consumers, Res. 1/2016: https://www.ila-hq.org/images/ILA/docs/No.1_Resolution_2016_ProtectionOfConsumers_4Models.pdf. One express example is article 2651 of the Argentinian Civil Code, it permits party-autonomy for all contract except to those involving consumers. Another is articles 89 e following of the Code of Private International Law of Panama which establishes a special regime for contracts where the parties are not in equal footing ("contratos desiguales o de adhesion").

83 There were intra-regional efforts to develop international conventions to deal international cross-border jurisdictional issues involving consumers, CIDIP VII is one of those initiatives. It was not fruitful because among other things there was no agreement on the role of party-autonomy and the availability of the option of chose arbitration as a means to settle disputes. For an overall view of the effort see: Fernández Arroyo, Diego y Moreno Rodríguez, José A. Protección de los Consumidores en America - Trabajos de la CIDIP VII (OEA). Asunción: La Ley-CEDEP, 2007. See also: http://www.oas.org/es/sla/ddi/docs/publicaciones_digital_XXXIV_curso_derecho_internacional_2007_Claudia_Lima_Marques.pdf; and https://docplayer.es/80967826-The-inter-american-convention-on-the-law-applicable-to-international-contracts-and-the-furtherance-of-its-principles-in-the-americas.html.

84 Retrieved from: http://www.oas.org/es/sla/ddi/docs/publicaciones_Contratos_Internacionales_OEA-ASADIP_2016_Publicacion_Completa.pdf.

9. Governments in the region are imposing stricter rules for content moderation and removal on online platforms

In the Internet & Jurisdiction Global Status Report 2019 it was identified that there is a global trend for states to have a tougher attitude towards internet platforms. Countries within the LAC region follow the same tendency.

Some countries in the region enshrined safe harbor protections for internet intermediaries in their legislations, creating a specific exception to the enforcement of general liability rules or general consumer protection regimes for the malfunction of products or services.[85] Even though the situation is rapidly changing and many local internet companies are springing up, countries in LAC are still served mostly by internet companies and platforms established outside the region. Thus, every interaction tends to be transnational, potentially raising jurisdictional issues.

> In Brazil, the Supreme Court has been called to rule on whether the safe harbor provision —a clause that limits the liability of internet intermediaries for hosting or transferring third-party content - present in the Brazilian Internet Bill of Rights is in accordance with the Federal Constitution. A bill to regulate intermediary liability failed to receive the necessary support in Argentina.[86] Similarly, Mexico has struggled to find support to establish a liability regime in accordance with the USMCA Agreement, which creates a safe harbor for cross-border digital trade amongst its parties.[87] In Ecuador, a bill was proposed to regulate speech online, including provisions that would make internet intermediaries directly responsible for taking down speech considered illegal.[88] A similar bill was proposed in Honduras as well providing wide-open definitions as to what is regarded as illegal speech that internet intermediaries should monitor.[89] A bill in Paraguay intended to impose obligations on ISPs to take down speech deemed "offensive".[90]

Civil society organizations have expressed their concern regarding initiatives to strengthen the responsibility of intermediaries.[91] The Inter-American Rapporteur for Freedom of Expression has also joined in echo to state potential risks for human rights of these legislative initiatives.[92]

85 Only Chile and Brazil have "safe harbor" provisions - that limit the responsibility of internet intermediaries -for hosting or transferring third-party content - enacted as part of their legislation. See: IDB, Accelerating-Digital-Trade-in-Latin-America-and-the-Caribbean: https://publications.iadb.org/publications/english/document/Accelerating-Digital-Trade-in-Latin-America-and-the-Caribbean.pdf.

86 Retrieved from: https://www.lanacion.com.ar/tecnologia/los-intermediarios-internet-debate-seguira-pendiente-nid2192063.

87 Retrieved from: https://www.derechosdigitales.org/12564/usmca-y-el-futuro-de-internet/.

88 Retrieved from: https://www.eluniverso.com/opinion/2017/06/13/nota/6229435/redes-sociales-censura.

89 Retrieved from: https://www.accessnow.org/comunicado-ley-que-regula-los-actos-de-odio-y-discriminacion-en-internet-de-honduras/; and https://www.hrw.org/news/2018/04/09/honduras-cybersecurity-bill-threatens-free-speech.

90 TEDIC. (2017, octubre 11). Un proyecto de Censura Política. Retrieved on September 26, 2019, from TEDIC website: https://www.tedic.org/un-proyecto-de-censura-politica/.

91 https://www.derechosdigitales.org/internetesnuestra/desafios-gobernanza.pdf.

92 OSCE, OAS, UN, ACHPR Joint Declaration on freedom of expression and "fake news", disinformation and propaganda Retrieved from: https://www.osce.org/fom/302796. The Inter-American Commission on Human Right has shown its concern as well with such similar initiative in the electoral context, see: https://www.oas.org/es/cidh/expresion/publicaciones/Guia_Desinformacion_VF.pdf.

10. Internet of Things knows no border and demands standardization

The Internet of Things (IoT) is more than providing internet connection: it creates technology-based *ecosystems* whose value stems from capturing, recording, and analyzing data. The implications of these functions are enhanced by their combination with cloud computing, blockchain, robotics and artificial intelligence.[93]

Business models revolving around IoT do not have to respect economic verticals and do not need to be restricted by national boundaries. They benefit from the borderless nature of the internet to which they are connected and to some extent to the dematerialization that comes with digitalization. This means a "sensor" society, where everything that can be linked to the internet will be and data that can be shared will be as well. Cross-border trade and trans-border data flows are a likely consequence of implementing IoT. To take full advantage of IoT, there is a need for scale, convergence, harmonization, and an interoperable environment with an interconnected market.

Stakeholders surveyed point out that the key challenges relate to the establishment of protocols, common standards, industry patterns, and the harmonization of rules and regulations. Their concerns for the region mostly coincide with the ones gathered in the Internet & Jurisdiction Global Status Report 2019: security and privacy; common technical standards; levels of product safety; availability of bandwidth and connectivity; rules on liability; and regional interoperability.

One stakeholder noted that full harmonization of regulations and standards within the region may be a hard goal to achieve, yet an agreement on rules or guidelines on how companies and states may navigate the regulatory differences across LAC is manageable. Some of the stakeholders emphasized that structuring a system around incentives for private investment should be the priority to allow the industry to operate across countries. All such concerns and suggestions showcase a need for intra-region and global coordination and cooperation.

11. Experts are divided on the need for specific IoT regulation

The opportunities of IoT relate to all areas that can have a sensor and that can be connected to the internet, from the most intimate (human bodies) to the most public (cities) passing through houses, industries and fields.[94] The cross-cutting nature of IoT means that opportunities and challenges rest in a vast array of themes and sectors.

Taking into consideration that providers may have a global reach,[95] cooperation and coordination seem to be paramount. Most initiatives have taken the form of national plans, strategies and policies. The majority have only marginally incorporated a global or regional dimension, failing to establish a link between these dimensions and the topic of IoT itself. Surveyed stakeholders agree on the need for harmonization, yet they seem to be divided on whether specific rules for IoT are necessary. For example, some question whether more underlying regulation such as consumer and personal data protection and cybersecurity should be interpreted extensively to encompass the challenges presented by this technology.

93 ECLAC, Data, algorithms and policies: redefining the digital world, 2018. Retrieved from: https://www.cepal.org/en/publications/43515-data-algorithms-and-policies-redefining-digital-world.

94 https://www.internetsociety.org/policybriefs/iot-privacy-for-policymakers/.

95 A study from McKinsey call attention to the global reach of certain service providers. Retrieved from: https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/unlocking-value-from-iot-connectivity-six-considerations--for-choosing-a-provider.

Plans, Strategies and actions:

Brazil has a National Internet of Things Plan, focusing on four main sectors: smart cities, health, agribusiness, and manufacturing. The plan also emphasizes four strategic areas of development: innovation and internationalization, human capital, regulatory safety and privacy, and infrastructure for connectivity and interoperability.[96]

Mexico has established as a policy priority to focus on the Industrial Internet of Things ("IIoT"). Car manufacturing is one of the focal points.[97]

Both Colombia and Argentina have developed —in partnership with the private sector— policies regarding IoT. Their focus is to incentivize strategic alliances, cooperation, and commercial agreements to foster an environment conducive to IoT development.[98]

12. There are several challenges and opportunities for smart cities in the region

Smart cities are another area where IoT plays a transformative role. This technology can be integrated into the city landscape in order to capture and analyze data so that authorities can, through traditional means or technological ones, better solve municipalities' problems.[99] IoT helps organize the urban setting, allowing for a faster and evidence-based response. Implementation is on its way for areas such as traffic, parking, security, pollution and hygiene.[100]

Thus, many international touchpoints are leading to potential jurisdictional complexities. Each layer, starting from the connectivity infrastructure (5G, for instance), is dependent on strategic alliances and cooperation between a series of suppliers and providers that may be established around the globe. As the IoT ecosystem in the region becomes more complex and goods and services are supplied through a chain of providers that may not be established in the same country as the user, jurisdictional solutions may have to be reviewed.

The LAC region has one of the highest levels of urban concentration, and the challenges are accordingly high. Thus, IoT for public services can have a significant impact and alter the whole panorama of a city and how public policies are designed for it. The cities themselves and the countries in the region alone cannot provide all the necessary solutions.[101] There is a tendency to foster partnerships and alliances with foreign providers, which makes the need for coordination even stronger.

96 In 2019 the plan was institutionalized though Presidential Decree n. 2984/2019. Retrieved from: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9854.htm. The original plan was issued in 2017 through a multistakeholder initiative in partnership with BNDES - the Brazilian Development Bank. Retrieved from: https://www.bndes.gov.br/wps/portal/site/home/conhecimento/pesquisaedados/estudos/estudo-internet-das-coisas-iot/estudo-internet-das-coisas-um-plano-de-acao-para-o-brasil.

97 Retrieved from: https://www.gob.mx/promexico/acciones-y-programas/mapas-de-ruta-22850.

98 In Colombia this was established through the "CEA-IoT" (Excellency Centre for Internet of Things). Retrieved from: http://www.cea-iot.org. In Argentina, the Chamber for Internet and IoT plays the same role. Retrieved from: http://cabaseiot.com.ar.

99 IDB, Big urban data: a strategic guide for cities, 2019. Retrieved from: https://publications.iadb.org/en/big-urban-data-strategic-guide-cities.

100 IDB, IoT IN LAC 2019: Taking the Pulse of the Internet of Things in Latin America and the Caribbean. Retrieved from: https://publications.iadb.org/en/iot-lac-2019-taking-pulse-internet-things-latin-america-and-caribbean.

101 IDB The road toward smart cities: migrating from traditional city management to the smart city, 2016. Retrieved from: https://publications.iadb.org/handle/11319/7743?locale-attribute=es&.

Argentina has a series of cities deploying IoT solutions.[102] Tigre, a city in the greater Buenos Aires, was one of the first municipalities in LAC to implement a safety and crime-combating "operation center" employing among others face and plate recognition cameras to track criminals and stolen cars. This initiative was achieved through a public-private partnership with multinational corporations and cloud data analysis.[103]

The city of Nassau, in the Bahamas, has developed a water management system that detects leakages, allows for advanced repair and replacement of pipes, controls pressure and manages different levels of measurement. This has allowed the municipality to cut costs and diminish water loss from 58% to 29%. [104]

13. Smart farming enlarges the set of international players and is a natural move for the region

Smart farming[105] and several AgTech (Agriculture startups) may present an important opportunity for the region. The deployment of IoT technology to the agriculture business can impact many verticals, such as management of crops, precision crop cultivation, monitoring of livestock, intensive vertical (indoor and outdoor) farming, better use of aquaculture. IoT for farms can have a positive impact on the whole value chain, improving both the decision-making and the efficiency and precision of the actions taken. Planting, monitoring, harvesting, distributing, storage, and marketing can be revolutionized.[106]

A significant part of the added value of IoT for agriculture comes from having access to data that otherwise would be very difficult to collect. Notable examples are humidity of soil and microclimate indicators. They may vary sharply. Deploying IoT technologies may make it easier to map out and monitor these indicators. The highest benefits stem from advanced analytics that are dependent on the scale and volume of data available and processing capabilities.[107] These two aspects might lead to services being rendered across jurisdictions and through partnerships with entities operating transnationally.[108]

The cross-border aspects do not end there. Much of these IoT solutions do not come from traditional agriculture sector companies, such as farmers or conventional suppliers such as farm equipment makers, seed suppliers, plant food, chemicals or seeds producers and suppliers, or even distributors. Software developers and predictive data analytics companies increasingly become part of agricultural or farm operations. Much of such non-traditional corporations are either not themselves necessarily based on the same country as the users (farms) or are assisted or part of an alliance or arrangement with off-country entities. One clear example is the usage of cloud services where in most cases, most of the companies are not in the region, nor the data is processed necessarily in-land.

102 An overview of the different initiatives of smart cities in Argentina is available at: https://www.camarabilbao.com/ccb/contenidos.downloadatt.action?id=5334087.

103 Retrieved from: https://www.nec.com/en/case/tigre/index.html.

104 IDB, The road toward smart cities: migrating from traditional city management to the smart city, 2016. Retrieved from: https://publications.iadb.org/handle/11319/7743?locale-attribute=es&.

105 Smart Farming is key for the future of agriculture, 2018. Retrieved from: http://www.fao.org/family-farming/detail/en/c/897026/.

106 Retrieved from: https://www.researchandmarkets.com/research/lv69c3/global_iot_in?w=4

107 Retrieved from: https://www.researchandmarkets.com/reports/4600903/iot-in-agriculture-market-outlook-and-forecasts#rela1-4669235.

108 In a study by the World Bank, such partnerships are singled out as crucial policies for the development of the sector. Retrieved from: http://documents.worldbank.org/curated/en/610081509689089303/pdf/120876-REVISED-WP-PUBLIC-Internet-of-Things-Report.pdf.

Notable developments and initiatives in smart farming

Rice farming in Colombia benefits from a project in partnership with a Japanese company. The IoT solution has sensors that collect environmental data such as air and soil temperature and humidity, and solar irradiance. This project enables both better decision-making and more efficient and timely responses.[109]

Livestock monitoring is also receiving attention. Checking the intake of water and animal feed constantly is necessary for such areas. In Brazil, a project in partnership with multinational corporations has made it easier to weigh livestock and analyze data on their growth.[110] Additionally, startups and traditional companies provide technology that monitors the geo-location of the herds and the health status of the animals.[111] Others manage the whole chain from "farm to table", adding sensors and agricultural intelligence to all processes.[112]

In Guanajuato, Mexico, a hub for AgTech has sprung up incentivizing a series of projects for business from the monitoring of crops to irrigation strategies.[113]

14. Digital payments in the LAC region coexist with an unbanked population, lower penetration of international cards, an enduring cash culture and foreign exchange volatilities

The internet has changed the landscape of many different businesses worldwide. The financial sector, more recently, is experiencing the consequences of this advancement.[114] New services and new business models are taking advantage of the connectivity of the online world to lower barriers to entry in the financial market, providing more products and services to a broader base of clients. Their virtual nature allows them not to be grounded in one country or the other, fostering and enabling cross-border transactions.

There is still, however, a significant gap between people that are served by traditional financial institutions and those that are not. A substantial portion of the population is either underserved or excluded from financial services. These gaps represent a significant hindrance to a Digital Single Market; people are either deterred from entering the market or simply are not capable of having access to it. Thus, goods and services supplied through the internet are also impacted: they become inaccessible or challenging to access for a relevant portion of the population.

In the LAC region this is reinforced by a higher than average percentage of the population still unbanked, a lower penetration of international cards, an enduring cash culture and foreign exchange volatilities. This presents an opportunity for entrants to

109 Retrieved from: https://www.e-kakashi.com/en/case/details01.

110 Retrieved from: https://blog.bosch-si.com/agriculture/connected-agriculture-beefed-up-networking-in-brazil/. A general study of its deployment in the south of Brazil can be found in here: https://www.lume.ufrgs.br/handle/10183/178439.

111 See for instance: Allflex (http://www.allflex.com.br/identificacao-eletronica/brincos-eletronicos-fdx/); Intergado, Cowmed and Imeve (https://www.beefpoint.com.br/o-olho-do-dono-que-engorda-o-boi-agora-e-digital/).

112 For instance, BovControl: https://www.bovcontrol.com; http://g1.globo.com/tecnologia/blog/startup/post/app-permite-a-fazendeiro-monitorar-bois-e-vacas-na-tela-do-pc.html.

113 Retrieved from: http://agrobioteg.org.

114 The World Bank and the International Monetary Fund (IMF) have sponsored the Bali Fintech Agenda underscore the opportunities and risks of innovative financial services providers, fintech. Retrieved from: https://www.worldbank.org/en/topic/fintech.

find fresh solutions and provide not only new products and services, but also boost inclusion in access to finance.[115]

15. Fintechs are revolutionizing financial services in the region, but face disparate regulatory treatment at the national level

The LAC region is experiencing a boom in companies that align new technologies with novel opportunities in the financial market.[116] There is extraordinary growth in the so-called *fintech* market [117]The initiatives have taken over different areas. Two have gained more momentum in the region: digital payments, supported by a growth in new banking enterprises (*neobanks*), and blockchain technologies, both in the form of cryptocurrencies and other potential applications that will be explored below.

Stakeholders interviewed and surveyed have highlighted this trend and the relevance that fintechs are having in the region. They have underscored their potential to diminish inequality of access to financial services and to take advantage of the digital market. Stakeholders noted however that harmonization initiatives may be rendered more difficult due to the difference in financial regulatory traditions in the region and the disparate size and nature of the countries' economies.

16. Cross-border jurisdictional aspects are increasingly impacting the activities of fintechs in the region

In the region, there are multiple digital payment and banking solutions. The market is moving towards novel solutions, which has motivated the creation of an ecosystem of companies that provide them.

> The LAC fintech environment is composed of hundreds of startups and new initiatives developed by more traditional actors.[118] In 2018, for instance, Brazil already had 380 fintech startups; Mexico, 273; Colombia, 148; Argentina, 116; and Chile, 84.[119] They range from a series of different activities. Among the most important are solutions related: to money transfers and management; international transfers and remittances; mobile points of sale; payment gateways and aggregators to accept, authorize, and process payments on digital platforms; and neobanks, technology finance entities possessing their own or third-party banking licenses.[120]

Several of these enterprises either offer trans-border services, for instance international remittances, or are themselves crossing borders by internationalizing their operations. Governmental initiatives are relevant to provide an institutional framework to foster growth

115 IDB, FINTECH: Innovations You May Not Know were from Latin America and the Caribbean, 2018. Retrieved from: https://publications.iadb.org/en/fintech-innovations-you-may-not-know-were-latin-america-and-caribbean.

116 IDB/Finnovisa, Report on Fintech in Latin America 2018: Growth and Consolidation. Retrieved from: https://publications.iadb.org/publications/english/document/Fintech-Latin-America-2018-Growth-and-Consolidation-final.pdf.

117 ECLAC, Data, algorithms and policies: redefining the digital world, 2018. Retrieved from: https://www.cepal.org/en/publications/43515-data-algorithms-and-policies-redefining-digital-world.

118 IDB, Fintech in Latin America. Retrieved from: https://publications.iadb.org/publications/english/document/Fintech-Latin-America-2018-Growth-and-Consolidation-final.pdf.

119 According to Finnovista, the numbers are even higher in 2020. Retrieved from: https://www.finnovista.com/tag/fintech-radar/.

120 IDB/Finnovisa, Report on Fintech in Latin America 2018: Growth and Consolidation. Retrieved from: https://publications.iadb.org/publications/english/document/Fintech-Latin-America-2018-Growth-and-Consolidation-final.pdf.

and to enable new financial solutions. Attempts to foster regulatory convergence could help secure regional and international markets for these enterprises. Yet, cross-border jurisdictional aspects should be taken into consideration to encourage and not hinder the process.

17. Experts reveal great enthusiasm for the adoption of innovative regulatory solutions, such as regulatory sandboxes

Regulatory sandboxes provide an opportunity for innovative solutions to operate for a restricted number of users (clients) and during a limited time. The initiatives often work with less stringent obligations under the condition that they will be continuously monitored and supervised by an authorized governmental organ.[121]

These sandboxes have the advantage of being testing grounds for new projects. They limit the impact and, consequently, the risks at the same time, allowing for the supervisory authorities to monitor the reactions of the agents and the market to propose specific approaches, standards and rules.

The majority of the stakeholders surveyed stated that such innovative approaches, such as regulatory sandboxes, help foster regional economic growth. They highlighted the differences in the economy of the countries in the region, the potential lack of institutional capacity, and availability of human resources as potential hindrances to the applicability of these regulatory solutions.

Some of the countries in the region are already deploying such solutions and may lead the way. For example, Mexico's law to regulate fintech companies[122] includes the possibility of temporary authorizations for "new financial models".[123] Similarly, in Colombia, the Superintendence of Finance has put in place a legal framework that allows the use of regulatory sandboxes for innovative financial initiatives. Brazil has regulatory sandbox initiatives[124] within the Central Bank[125] and the Securities Oversight Agency (CVM).[126] Industry Associations have put forward proposals as well, as it is the case of Fintech Ibero-America, an international federation of national associations aiming at creating a regulatory synergy in the region.[127]

121 IDB, Regulatory Sandboxes in Latin America and the Caribbean for the FinTech Ecosystem and the Financial System, 2018. Retrieved from: https://publications.iadb.org/en/regulatory-sandboxes-latin-america-and-caribbean-fintech-ecosystem-and-financial-system.

122 Law to Regulate Financial Technology Companies ("Ley para Regular las Instituciones de Tecnología Financiera"), March, 2018. Retrieved from: https://perma.cc/SB6N-RQY7.

123 Mexico's Fintech law. See: Kurc, C. & Portilla, A. (2019, May 10). Mexico: Fintech 2019. International Comparative Legal Guides. Retrieved from https://iclg.com/practice-areas/fintech-laws-and-regulations/mexico.

124 Retrieved from: https://forbes.co/2020/02/06/economia-y-finanzas/hacienda-cobijara-con-decreto-el-sandbox-de-la-superfinanciera/.

125 Retrieved from: https://www.centralbanking.com/fintech/4397616/sandbox-initiative-central-bank-of-brazil. A brief analysis proposing that it may be an innovative sectoral regulatory sandbox. See: https://www.jota.info/coberturas-especiais/inova-e-acao/banco-central-ganha-premio-de-melhor-iniciativa-de-sandbox-do-mundo-04092019.

126 On May 15, 2020, the CVM issued "Instrução" 626/2020 implementing regulatory sandboxes. Retrieved from: http://www.cvm.gov.br/noticias/arquivos/2020/20200515-1.html.

127 Retrieved from: http://fintechiberoamerica.com/wp-content/uploads/2018/06/protocolo_implementación_sandbox_iberoamerica.pdf.

These reflections highlight the necessity and the opportunity for cross-border cooperation and coordination. Countries in the region may benefit from their proximity and pool resources together. Setting common standards and approaches can facilitate the oversight work and diminish regulatory variation and, as a consequence, serve clients who are excluded or underserved by the traditional financial services sector.

18. Blockchain and cryptocurrencies as enablers of cross-border trade (and crime)

Blockchain is another technology being developed to facilitate transactions. Blockchain may be understood as a distributed ledger where records of peer-to-peer transactions are kept without the necessity of a central authority to coordinate it. Satoshi Nakamoto conceptualized the technology in 2008 to eliminate the usual trusted middleman involved in most transactions.[128] It provides a way to cope with uncertainty. The distributed nature of the ledger, its immutable (tamper-proof), and self-executing nature, make it unnecessary for the parties to know or trust each other. Trust becomes the result of the use of blockchain.[129]

The Internet & Jurisdiction Global Status Report 2019 has already highlighted the international interest with which both private and public sectors have welcomed this technology. The GSR 2019 however noted the healthy dose of skepticism some stakeholders, especially states, have had with specific applications, most notably cryptocurrencies. Indeed, Bitcoin has become widely known as one of such currencies. The legal challenges with such currencies and blockchain, in general, come from the same features that, in most cases, make them appealing: the lack of a focal, central authority and the fact that people do not have to know or trust each other.

The distributed and dematerialized nature of the ledger makes borders, and traditional jurisdictional elements significantly less relevant. Blockchain enables cross-border trade of all kinds without a necessary intermediary to oversee and inspect. Meaning, both legal and illegal transactions can flow without the knowledge of authorities and any necessary jurisdictional interpolation.

Discussions on blockchain and cryptocurrencies tend to focus, then, on potentially illegal contexts where transactions may occur. On the one hand, they may support criminal activities since they exchange hands easily, remotely and without reference to a controller. On the other, they seem anonymous because no information on the identity of the people participating in the transaction is recorded. Nonetheless, it does not necessarily mean that those involved cannot be identified. The blockchain protocol allows for traceability of all transactions, making it possible to recreate the whole path of the currency. In this sense, it is much less anonymous than hard currency, for which it is hard to retrace its steps once it exchanges hands.

Future discussions should clearly distinguish between cryptocurrencies and the generic technology of blockchain, which has many diverse potential applications.

[128] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf.

[129] ECLAC, Data, algorithms and policies: redefining the digital world, 2018. Retrieved from: https://www.cepal.org/en/publications/43515-data-algorithms-and-policies-redefining-digital-world.

Regional Noteworthy Cases and Initiatives:

The Eastern Caribbean Central Bank (ECCB) has developed a pilot program to facilitate compliance with international money laundering and terrorism's finance report regulations and has developed a "blockchain-based currency" available to multiple states across the Caribbean.[130]

In 2018, Venezuela announced a plan to launch an oil-backed cryptocurrency called "Petro". The plan was to issue 100 million Petro tokens (at an equivalent price of US$6 billion) with the intention that this would facilitate international transactions, diminishing reliance on currencies such as the dollar or the Euro.[131]

130 Retrieved from: https://www.eccb-centralbank.org/news/view/eccb-to-issue-worldas-first-blockchain-based-digital-currency.
131 Retrieved from: https://www.washingtonpost.com/news/worldviews/wp/2018/02/20/venezuela-launches-the-petro-its-cryptocurrency/.

A. Legal Trends

States in the LAC region vary on the degree to which they employ legal solutions to perceived issues related to the regulation of the internet. There is an overall growing trend to expand the applicability of national laws to situations beyond the countries' defined physical borders. It is becoming more and more a standard to ascertain adjudicative jurisdiction based on what is called 'effects doctrine' or on a 'targeting test'. Courts have issued orders to takedown (and/or stay-down) and stay-up online content. There is as well an emphasis on coupling regulation applicable to the internet with high fines and sanctions. Terms of Service and community guidelines created by major international internet platforms are also playing an increasingly important role and assume even more foundational aspects to guide behavior online.

1. States are increasingly resorting to an "effects doctrine" in asserting jurisdiction

There is a broad trend for states to assert jurisdiction to conducts and activities whose origin lies in another state or territory whenever they have a substantial connection to the country asserting it. This connection tends to be understood in relation to the activity of targeting consumers, doing business, causing harm, or affecting in a concrete way people or assets located within the borders of a country.

Most cases in the region tend to straightforwardly state its jurisdiction based chiefly on the place where the harm was felt, such as place of residency of the victim or location of their business. Such a targeted approach is also seen in some pieces of legislation, including Argentinian, Brazilian,[132] Colombian,[133] Mexican,[134] and Peruvian[135] data protection legislation. Another example is the Venezuelan Special Law Against Computer Crime.

2. The expansive scope of jurisdiction may not lead to its actual enforcement

A significant number of the surveyed stakeholders called attention to the fact that there is an imbalance of power and that even if many countries are implementing legislation with an extraterritorial scope, not all states are capable of enforcing such laws. A few have highlighted as well that within regional agreements such types of regulation may more effectively play a role, yet it is still very challenging to find common ground.

[132] Translation to English retrieved from IAPP website: https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf.

[133] Colombia, Law 1581, 2012, "Provisions for the Protection of Personal Data". Retrieved from: https://www.defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_1581_2012.pdf.

[134] Mexico, Federal Law for the Protection of Personal Data Held by Private Parties (Ley Federal de Protección de Datos Personales en Posesión de los Particulares), 2010; together with Regulations to the Federal Law on the Protection of Personal Data held by Private Parties (Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares) from December, 2011, and Privacy Notice Guidelines, from January, 2013.

[135] Peru, Law 29.733, 2011, "Law on the Protection of Personal Data".

Lacking the actual capability of constraining the parties to comply may lead to diminished legitimacy of the regulation. Such approach has been criticized as well for: (i leading to arbitrary enforcement —too many potential non-compliant actors, since one has to choose which to pursue; (ii for eroding legal certainty —too many not prosecuted leads to an understanding that the law is not applicable; and (iii for potential trans-border compliance conflicts —norms from two or more countries may require different actions concerning the same conduct, leading to conflicts and obliging entities to choose which law to comply with.

3. Higher courts in the region have so far refrained from decisions with a global reach

One surveyed stakeholder mentioned that in Latin America higher courts have so far restrained themselves and have not issued orders with a global reach on issues concerning the internet. Another was of the opinion that the interpretation of the potential global scope of individual online rights has not yet been determined in many countries in the region.

The cases of de-listing provide some nuance to this issue. In the Court of Appeals of the State of São Paulo, in Brazil, for instance, there are cases in which the Court has ordered Google Brasil to de-list search results from its website or to remove videos from YouTube on a global scale. The very same Court, in other cases, has questioned how its rulings could affect other jurisdictions. On the case *Centro Espírita Beneficente União do Vegetal vs. Google Brasil Internet Ltda,* the judge has stated that "[...] this court does not have jurisdiction to determine if the video indicated in the Plaintiff's briefing is also available in other countries, such as Colombia and Germany, under penalty of transferring the scope of its competence and incurring a violation of the sovereignty of other countries."[136]

4. National courts are increasingly ordering platforms to takedown, stay-down and stay-up content posted online

There is a global trend reflected as well in the LAC region towards court orders requiring platforms to takedown, stay-down and stay-up content posted online. The disparity in consensus towards the standard of protecting different rights, particularly free speech, is a major source of cross-border disputes.

As a legal trend, takedown orders are the most common. They are usually issued in connection to tort proceedings requesting monetary compensation. The relief aims at prohibiting the content from continuing to be exhibited. Yet, they may have other specific aims, such as taking down information that is misleading or that may damage someone's reputation.

It is rather common that such orders have trans-boundary elements: the platform is foreign in origin, the technique used comes from overseas, data is in offshore servers. A vast array of situations make many of such orders touch upon matters outside the territory of the country where they originate.

Stay-up decisions, as yet, are not as common; very few countries have issued them. Often the understanding concerning freedom of expression online is that platforms have to respect freedom of speech. Yet, they have some leeway to enforce some restrictions, mainly based on their Terms of Service and community guidelines.

136 Tribunal de Justiça do Estado de São Paulo. Centro Espírita Beneficente União do Vegetal vs Google Brasil Internet Ltda; 11.08.2016 <https://www.conjur.com.br/dl/justica-local-nao-obrigar-google2.pdf>.

5. In addition to civil liability, countries are increasingly resorting to administrative sanctions to foster compliance with sectorial norms

Administrative sanctions imposed by local authorities are an important tool to enforce internet-related regulation. The authorities might vary depending on the specific issue at hand, such as consumer protection, antitrust, environmental, or data protection. The sanctions usually range from warnings, fines, suspension, or termination of a particular activity.

As described in previous sections, many of the data protection regulation in the Region was inspired by the European legal framework, which provides severe administrative sanctions. One notable difference, however, is that the European regulation provides for international cooperation among the countries, while in the ECLAC Region, most of the rules concerning administrative liability are drafted with a national scope.

6. Terms of Services have interlocked with national laws, reinforcing or disputing the status of a user's behavior

Terms of Service, created by multinational companies, have interlocked with national legislations in some ways serving as a major source of guidance on what is allowed and what is not on such platforms. On one side, they face the challenges of balancing freedom of expression against potentially harmful speech. On the other, they have to take stock of significant changes to the legal landscape in areas such as intellectual property, data privacy, liability limitations, and consumer protection.

A major cross-border aspect deals with the fact that such platforms tend to be built on top of a world-wide or at least regional architecture. Thus, many elements of the Terms of Service that support such architecture have a common core. Standards developed by the platforms cover vast areas of the globe and impact accordingly. National regulatory and customary standards may clash with such terms and guidelines, causing the need for accommodation.

7. Impacts of the controversial update of the European Copyright Directive can already be felt in the region

The EU has updated its Copyright Directive, creating incentives for platforms to provide mechanisms for content moderation —even before it is published. This Directive has had an impact on countries in the Region. A few have launched proceedings to reform their IP legislation. Brazil, for instance, has embarked on a consultation and started an extensive study on a new national strategy on intellectual property. One of the topics refers to mechanisms of protection against online piracy and is heavily inspired by the latest developments in European Law.

8. Online marketplaces are deploying dispute resolution systems as governments push for co-regulation on the sale of counterfeit goods

Certain governments in the LAC region have been pressuring or even entering into agreements with e-commerce platforms to improve their actions against piracy and selling of counterfeit goods. These actions have led many e-commerce platforms to self-regulate and add non-judicial means of dispute resolution to their terms and conditions. They use in-house means (automatic more often than not) to find and take down perceived violations (counterfeit or pirate). The alternative dispute mechanisms usually provide an opportunity for both the owner and the accused violator to express their views.

In addition to dispute resolution systems set up by the private sector, governments in the region have been fostering co-regulation initiatives. These initiatives are inspired by the Memorandum of Understanding on the sale of counterfeit goods via the internet, facilitated by the European Commission and agreed by several platforms, right owners and associations.

9. For the sake of consumer protection, courts in the region tend not to uphold choice of forum and choice of law clauses in Terms of Service of international internet platforms

In many instances, Terms of Service define the forum to settle disputes and the applicable law. They are considered contracts (even if "adhesion contracts") regulating the relationship with its users and such clauses as party autonomy. In the region, however, the tradition of consumer protection is robust, and there is a perception that party autonomy should be limited, particularly in circumstances where a consumer is involved and cannot negotiate the clauses of the contract. This reflects an upcoming trend identified in the Internet & Jurisdiction Global Status Report 2019 of not upholding choice of forum and choice of law clauses in Terms of Service of international internet platforms.

B. Major Technical Approaches

The LAC Region is no exception to the rule that several of the most important legal issues related to internet and jurisdiction tend to be approached through the lens of technical solutions. A variety of them follow similar lines as other countries in the world, yet some of them end up having a very particular regional flavor. This section intends to showcase and analyze the most significant of such technical approaches that appear in the region and highlight the peculiarities that have developed among the LAC countries. The analysis has been made through a lens related to the trans-border impacts they may have and their practical and legal implications.

1. The use of personal data to map and control the Covid-19 pandemic will consolidate the discussion about geo-location technologies in the region

In many places around the world, the debate on the usage of geo-location technologies has matured in the last two decades. In Europe more than most, the debate started with a discussion on the possibility of deploying such techniques, based on their level of accuracy, and has evolved with a focus on their appropriateness and the extent of their use. The European Union, alongside policies to constitute a European Digital Single Market, has even issued Regulation 2018/302 concerning geo-blocking, one of the potential functions of geo-location technologies.

In the LAC region, the level of discussion on geo-blocking has not reached the regulatory specificity of other countries and regions. Yet, under the heading of consumer and data protection, there is a blooming political and legal debate on the implications, particularly of geo-location technologies, especially geo-blocking and geo-pricing.

As the fight against the Covid-19 pandemic lingers, countries in the region are trying to resort to more data to address the spread of the virus better. Geo-location technologies are increasingly playing a role in determining the degree of social distancing adopted by a larger group or mapping the routes and contacts of infected individuals.

Concerns over privacy and data protection are growing as the trans-border nature of the internet makes it easier for sensitive data to be stored in a foreign country. Additionally, countries with a recent history of authoritarian regimes are facing public demonstrations from individuals that claim that the usage of geo-location data to fight the pandemic is an excuse for installing unprecedented control over the citizens.

One can expect that a more informed debate over the use of geo-location technologies, intertwined with political, legal, and technical concerns, will only mature in the region as a legacy of the fight against Covid-19.

2. Geo-blocking and geo-pricing are raising concerns over antitrust, consumer and data protection

In Brazil, for instance, the online travel company despegar.com has been fined for both geo-blocking and geo-pricing its customers. The case concerned discriminating customers from Brazil and Argentina as some hotels were offered with average prices higher for Brazilian customers than for Argentinian ones. Additionally, the company would block access to specific hotels and services (renting certain cars) for customers of one country and not the other.

3. Content filtering is on the rise as countries fight hate speech and disinformation in the region

Hardly any country in the LAC region has organized its network to *a priori* block (or filter) incoming content or police nationally produced content. Such restrictions have not been installed as part and parcel of the network in the LAC countries' infrastructure. Yet, many governments have sought to impose an obligation on the access providers or the internet service providers to monitor, filter, or takedown certain categories of content in a short period of time.

The Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights has analyzed the institutional architecture that restricts and filters content available online in Cuba. It has noted a few pieces of regulation that stand out. It is worth mentioning Resolutions N° 127/2007 - regarding Security for Information Technologies - and N° 179/2008 - Regulation for Internet Service Providers concerning public access to the internet. The former forbids the circulation of data or information contrary to the "social interest, public morals and mores". The latter imposes obligations on the ISPs to monitor and "regulate" content online and establishes a regime of direct responsibility for intermediaries.

In Venezuela, the Law on Social Responsibility on Radio, Television, and Electronic Media (the Resorte-ME law) establishes that ISPs may be held liable for information made available that i.e. "promotes anxiety among the citizenry, disregards legitimately of constituted authorities, incites the alteration of the public order, disseminates or encourages noncompliance with existing laws".

Some countries have pushed for legislation that would require service providers to deploy mechanisms that identify and, in certain cases, take down speech containing disinformation, particularly during elections. The Special Rapporteur on Freedom of Expression has declared that under the Inter-American standards any regulation that would require ISPs to deploy any content blocking or filtering, should be restricted to only exceptional cases such as child pornography, war propaganda and hate speech - that constitute incitement to violence or incitement to genocide, with the additional protection that an independent judge determines the illegality of the content.

4. App blocking has changed from a last resort to a common practice in the region, with impacts across borders

Due to the architecture of the internet and its interconnected nature, a shutdown in one place may impair access or usability in another. If the shutdown is orchestrated on the infrastructure layer of the internet, it is even more likely that it will have repercussions that go beyond the original intended territory. Users as well may not be restricted inside the borders of one country, and services may be provided through a transnational matrix.

Countries of the LAC Region are no different. One interviewed stakeholder noted that in the region, the internet infrastructure is shared by many countries and companies. An action in one part may have repercussions on others even across different states. In many cases, governments, courts and companies have blocked certain internet services, and apps leading to consequences felt beyond the intended target area or service. Another stakeholder mentioned that what was once a last resort tactic, has now become common practice.

In December 2015, a Brazilian judge ordered the instant messaging service application WhatsApp to be blocked for 48 hours due to a refusal to hand over communication data on ongoing criminal investigations. This was not an isolated case, as two other court orders blocking the same application followed suit in different states of the country. All judicial orders were quickly reversed. Yet, the matter is still pending a decision on two constitutional cases in the Brazilian Supreme Court. These cases address the extent of the powers of judges to order such blocks and the allegation of the technical impossibility of access to the data due to the end-to-end encryption used by the messaging service.

The blocking was issued for the telecommunication carriers that complied with shutting down access at the infrastructure level. It was reported that users of the app in Argentina and Chile were also impacted and could not access the service either.

In October 2019, concomitantly to protests in Quito due to President's Lenin Moreno publication of Decree 883, instating austerity measures, it was reported that in Ecuador certain messaging and multimedia exchanging services such as Facebook and WhatsApp were not available.

On April 13, 2016, a court order in the city of Buenos Aires (Argentina) required the car-sharing platform Uber to stop its activities there. ISPs were instructed to shut down Uber's mobile application and online platform. Not only was the service of the multinational corporation interrupted in the city of Buenos Aires, but the affected area went beyond the intended borders of the capital.

On November 14, 2019, the Ministry of Telecommunications and Transport (MTC) of Peru issued the Decree 035/2019, providing powers to block transportation apps deemed to offer illegal services – including bicycles, taxis, and e-scooters – unilaterally and without a court order. It is reported that the Ministry requested ISPs to block certain apps and that it had requested Apple and Google app stores to stop displaying such transportation apps.

5. Some governments order DNS blocking in the region, but it is not a widespread practice

Some governments in the region are known for practices of DNS blocking, although this measure is not widespread in the region as a whole. Recently, the Venezuelan Government blocked the Tor network, a tool that allows users to browse the internet anonymously. The blocking was executed by the government-owned internet service provider CANTV, the largest ISP in the country.[137] In order to access the blocked tool, Venezuelan users had to rely on virtual private networks (VPNs) to circumvent government regulation.

In Cuban "parknets" (the name given to public spaces to access the internet), several websites have been reportedly blocked, including media outlets.[138]

6. Internet shutdowns are not common in the region but might happen during times of social unrest

Internet shutdowns are a voluntary disruption of internet access for short periods, mandated by local authorities, usually in situations of threats to public order —real or alleged. They may have destabilizing consequences, as they not only prevent communication but also access to information. Without access to the internet, a population's ability to realize many daily activities is obstructed. Populations can find themselves unable to communicate online, research and have access to even basic services (some of them public).

As financial transactions are migrating more and more to the internet, thus access to money and different resources may also be disrupted. More lasting consequences relate to consumer confidence and the need for businesses to migrate to more costly alternatives due to the instability of the network.

In Venezuela, for instance, not only app and internet services blockings have occurred, but also shutdowns or disruption of internet connectivity to entire areas for short periods of time. Such instances tend to be connected to significant political events. In 2019, internet shutdowns or large disruptions to connectivity were reported to have occurred multiple times - particularly with the state internet provider. They were related in most cases to political activities by Juan Guaidó (President of the Venezuelan National Assembly and self-proclaimed President). One noticeable situation of internet shutdown reportedly occurred during a meeting of Juan Guaidó and the President of Colombia in their countries' border.

Regional human rights institutions such as the Inter-American System of Human Rights, through its Special Rapporteurship for Freedom of Expression has condemned shutdowns and internet disruptions. Such actions, when taken by governments or under governmental orders, are seen as "extreme measure[s] analogous to the prohibition of a newspaper or a radio or television station. Such blockades or restrictions cannot be justified, not even for reasons of public order or national security and cannot be used as censorship measures or as mechanisms to prevent access to information of the population."

137 https://www.accessnow.org/venezuela-blocks-tor/.
138 https://blog.torproject.org/measuring-internet-censorship-cubas-parknets.

7. Mandatory data localization is adopted in some countries for different reasons, but it raises serious concerns among stakeholders

Several countries in the region have debated, and some mandated the storage of data locally. The most important arguments for such forced localization of data tend to relate to national security, national safety and law enforcement access to relevant data. The logic is that data stored in servers within the territory are more readily available under the state's jurisdiction, thus, providing more security and control.

> Following the scandals of the Snowden revelations back in 2013, when data related to high officials of many countries was accessed, leaked of handed over to US' National Security Agency, several administrations in the region have considered mandating that at least some particularly sensitive data be stored in servers within their territory.
>
> One very significant example is an amendment suggested to the so-called Brazilian Internet Bill of Rights ("Marco Civil da Internet). A Parliamentary amendment to the bill intended to mandate data location in a very generic way. The amendment's wording is as follows: "The Executive Branch, through Decree, may force connection providers and Internet applications providers provided for in art. 11, who exercise their activities in an organized, professional, and economical way, to install or use structures for storage, management, and dissemination of data in the country, considering the size of the providers, its sales in Brazil and breadth of the service offering to the Brazilian public."
>
> The proposal was declined, but, as approved, the law specifies that Brazilian Law is applicable when companies, even foreign ones, offer services to the Brazilian public.

On the other side of the spectrum, Mexico signed an agreement with the US and Canada (The United States, Mexico, and Canada Trade Agreement - USMCA), in which among its clauses on digital trade, there is one preventing any legislation that would require the localization of servers within its jurisdiction.

Out of the surveyed stakeholders, more than 70%, strongly agree or agree that compulsory data localization restricts the free flow of information and international trade.

A number of stakeholders in their comments mentioned that it is only natural for a global networked economy to have data flowing across borders unimpeded and that obligatory data localization restricts and clusters the internet. As a technical matter, one of the stakeholders called attention to how compulsory data localization may impact the velocity of the network and the quality of the services. Costs may be felt not only in terms of higher prices but also in the potential for innovation. One interviewed stakeholder voiced concern that such obligations restrict the scale that smaller players might have as only the biggest players will be able to afford the infrastructure costs to maintain servers in different countries.

GLOSSARY

The policy coherence needed to build a thriving and integrated regional digital ecosystem demands the very same coherence in the definitions that shape the debate. The Internet was created more than 50 years ago. The World Wide Web is beyond its 30th anniversary. As some concepts have matured throughout the years, serving as well-known entry points for policy discussion, some are still very contentious as they try to grasp the essential aspects of new technological trends. This short glossary aims at bringing new actors in the field up to speed with key concepts that are mentioned in the report, adding clarity to the trends and to the legal and technological solutions mentioned therefore.

1. **Internet** is the global system of interconnected computer networks that rely on the Internet protocol suite (TCP/IP) to communicate between networks and devices.

2. **IP** *(Internet Protocol)* is "the communications protocol underlying the Internet, allowing networks of devices to communicate over a variety of physical links. Each device or service on the Internet has at least one IP address that uniquely identifies it from other devices or services on the Internet."[139]

3. **World Wide Web** *(WWW)* is an information system where documents and other resources are interlinked by hypertext and are accessible over the Internet, making it "easy for anyone to roam, browse, and contribute to."[140]

4. **DNS** *(Domain Name System)* is the naming system that "helps users to find their way around the Internet." As every computer on the Internet has a unique address, consisting of a string of numbers (the "IP address"), the DNS makes using the Internet easier by allowing a familiar string of letters (the "domain name", like www.internetjurisdiction.net) to be used instead of the IP address.[141]

5. **Jurisdiction** has different meanings in international law. In this Report it is used to signify the power to hear and/or to take decisions regarding a specific matter, by an authority or a formally constituted legal body. It is usually related to the idea of territory, but these two concepts are not always associated. That is particularly true when it comes to internet related topics, due to the cross border nature of the internet.[142]

   As previously remarked in the Internet & Jurisdiction Global Status Report 2019:

   "A distinction is often drawn between personal jurisdiction and subject matter jurisdiction. Personal jurisdiction relates to a court having jurisdiction over a particular legal or natural person. Subject matter jurisdiction relates to whether a court has jurisdiction over the type of dispute in question. Recent litigation, however, has brought attention to a third type of jurisdictional issue: 'scope of jurisdiction'. Scope of jurisdiction relates to the geographical scope of orders rendered by a court that has personal jurisdiction and subject-matter jurisdiction.

   This issue —which overlaps with the law of remedies— has lately arisen with courts making global blocking, de-referencing or content removal orders. Considerations as to the appropriate scope of jurisdiction are intrinsically linked to the strength of the relevant claim of personal jurisdiction, as well as to the choice of law. For example, where a court has a relatively weak claim of personal jurisdiction, it may not be in a position to opt for an expansive scope of jurisdiction. A court opting for an expansive scope of jurisdiction may also not be able to apply only its own law, given the impact its judgment will have abroad."[143]

---

139 Retrieved from: https://www.icann.org/resources/en/glossary.
140 Retrieved from: https://www.w3.org/WWW/.
141 Retrieved from: https://www.icann.org/resources/en/glossary.
142 See further: Svantesson, D. (2017). Solving the internet jurisdiction puzzle. Oxford, United Kingdom: Oxford University Press, 14-25.
143 Retrieved from: https://www.internetjurisdiction.net/news/release-of-worlds-first-internet-jurisdiction-global-status-report.

6. **Choice of law** is the ability of contractual parties to choose which law will govern eventual disputes between the parties and the contract's interpretation. The Report addressed this concept when referring to the choice of law clause usually included in Terms of Services and community guidelines of international internet platforms. In this type of online agreements, 'party autonomy' in choosing this law is usually questioned, as the user faces unilaterally predetermined contractual terms.

7. **Encryption** is "the process of encoding data so that it can be interpreted only by intended recipients."[144] It is used as a key security and privacy feature by several popular applications, from e-commerce to internet banking, from instant-messaging to video communications apps.

8. **Blockchain** is "a shared ledger of transactions between parties in a network, not controlled by a single central authority." The blockchain "works like a record book as it records and stores all transactions between users in chronological order. Instead of one authority controlling this ledger (like a bank), an identical copy of the ledger is held by all users on the network, called nodes."[145]

9. **Financial technology** *(abbreviated fintech or FinTech)* refers to entities that specialize in providing financial services chiefly through technologically enabled online platforms.[146]

10. **Regulatory Sandboxes** are spaces provided for companies to experiment with the operation of innovative products or services in a limited fashion with less stringent rules under the supervision of a regulatory governmental authority.[147]

11. **Fake News** is a term that served in the last decade as a politically biased label to refer to any "false and misleading information, disguised and disseminated as news".[148] The academic debate over a more appropriate term is still ongoing, with authors suggesting the use of definitions such as "disinformation" or "misinformation". In that sense, disinformation can be defined as "false information that is deliberately created or disseminated with the express purpose to cause harm. Producers of disinformation typically have political, financial, psychological, or social motivations." Misinformation, on the other hand is "information that is false, but not intended to cause harm. For example, individuals who don't know a piece of information is false may spread it on social media in an attempt to be helpful."[149]

12. **Deepfake** is a term currently used to describe fabricated media produced using artificial intelligence. By processing elements from previous video or audio files, "it enables the creation of a new content in which individuals speak words and perform actions which are not based on reality".[150] As the technology evolves, it is likely that deepfake will be increasingly used in disinformation campaigns.[151]

13. **Internet of Things** *(abbreviated IoT)* is a system of interrelated devices with the ability to collect and transfer data over a network without requiring human continuous interaction. In a more complex scenario, IoT can be defined as "a self-configuring, adaptive, complex network that interconnects 'things' to the Internet through the use of standard communication protocols. The interconnected things have physical or virtual representation in the digital world, sensing/ actuation capability, a programmability feature and are uniquely identifiable. The representation contains information including the 'thing's' identity, status, location or any other business, social or privately relevant information. The 'things' offer services, with or without human intervention, through the exploitation of unique identification, data capture and communication, and actuation capability. The service is exploited through the use of intelligent interfaces and is made available anywhere, anytime, and for anything taking security into consideration."[152]

144 Retrieved from: https://firstdraftnews.org/wp-content/uploads/2018/07/infoDisorder_glossary.pdf?x25702.

145 Retrieved from: https://www.oecd.org/finance/OECD-Blockchain-Primer.pdf.

146 For further information see: Magnuson, W. J. Regulating Fintech, 2017. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3027525.

147 Retrieved from: https://publications.iadb.org/publications/english/document/Regulatory-Sandboxes-in-Latin-America-and-the-Caribbean-for-the-FinTech-Ecosystem-and-the-Financial-System.pdf.

148 Retrieved from: https://en.unesco.org/sites/default/files/journalism_fake_news_disinformation_print_friendly_0.pdf.

149 Wardle, C. & H. Derakshan (September 27, 2017) Information Disorder: Toward an interdisciplinary framework for research and policy making, Council of Europe, https://rm.coe. int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c.

150 Retrieved from: https://firstdraftnews.org/wp-content/uploads/2018/07/infoDisorder_glossary.pdf?x25702. For further information see: Yuezun Li et al., "In Ictu Oculi: Exposing AI Generate Fake Videos by Detecting Eye Blinking," June 2018. https://arxiv.org/pdf/1806.02877.pdf.

151 For further information see: https://www.lawfareblog.com/deepfakes-looming-crisis-national-security-democracy-and-privacy.

152 Retrieved from: https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf.

ACKNOWLEDGEMENTS

Authorship team:

AUTHOR:

Carlos Affonso de Souza
Rio de Janeiro State University (UERJ)
Director - Institute for Technology & Society (ITS Rio)

RESEARCH ASSISTANCE:

Christian Perrone
Ph.D. Candidate - Fulbright Scholar
Senior Researcher - Institute for Technology & Society (ITS Rio)

Giovana Carneiro
Junior Researcher - Institute for Technology & Society (ITS Rio)

Project coordination (I&JPN):

Martin Hullin
Director of Operations and Knowledge Partnerships
Secretariat of the Internet & Jurisdiction Policy Network

PROJECT TEAM (I&J Policy Network):

Bertrand de La Chapelle
Executive Director
Secretariat of the Internet & Jurisdiction Policy Network

Paul Fehlinger
Deputy Executive Director
Secretariat of the Internet & Jurisdiction Policy Network

PROJECT TEAM (UN ECLAC):

Edwin Fernando Rojas
Division of Production, Productivity and Management
Economic Commission for Latin America and the Caribbean

Alexis Arancibia
Consultant, Economic Commission for Latin America and the Caribbean

Alonso Zuñiga Irigoin
Consultant, Economic Commission for Latin America and the Caribbean

PRODUCTION:

United Nations Economic Commission for Latin America and the Caribbean
Secretariat of the Internet & Jurisdiction Policy Network, Paris, France

EDITING:

Sophie Tomlinson
Manager, Communications and Outreach
Secretariat of the Internet & Jurisdiction Policy Network

We greatly appreciate the time and contribution of all participating survey respondents and interviewees. Without their valuable insights, this report could not have been produced.

Mauricio Agudelo
Director - CAF Development Bank
Colombia

Pablo Bello
Head of Private Messaging Policy LATAM - Facebook
Brazil

Daniel Cavalcanti
Coordinator - Ministry of Science, Technology, Innovations and Communications
Digital Policies Secretariat
Brazil

Maria Angélica Chinchilla Medina
Director of Telecommunications Evolution and Market
Ministry of Science, Technology and Telecommunications (MICITT)
Costa Rica

Jose Clastornik
President of GovTech Uruguay - Former Executive Director
National Agency for e-Government and Information Society (AGESIC)
Uruguay

Pelayo Covarrubias
President - Pais Digital
Chile

Agustina Del Campo
Director - Center for Studies on Freedom of Expression (CELE)
Argentina

César Díaz
Engineer
Uruguay

Lester García
Head of Connectivity Policy LATAM - Facebook
Mexico

Raúl Echeberría
Director - RCE - Digital Development Consulting
Uruguay

Alexandre Fernandes Barbosa
Manager - Regional Center for the Development of Information Society (CETIC)
Brazilian Network Information Center NIC.br
Brazil

Matias Fernandez Diaz
Senior Manager (Public Matters) - Mercado Libre
Argentina

Gustavo Gómez
Executive Director - Observacom
Uruguay

José Juan Haro
Head Regulation - Telefonica
Spain

Héctor Huici
Former Secretary - Information and Communication Technologies Secretariat
Argentina

Erick Iriarte
Partner - IALaw
Peru

Juan Jung
Director - Centro de Estudios de Telecomunicaciones de América Latina (cet.la)
Uruguay

Yacine Khelladi
Regional Coordinator, Latin America and the Caribbean - Alliance for Affordable Internet (A4AI)
Dominican Republic

Juan Carlos Lara
Content Director - Derechos Digitales
Chile

Carolina Limbatto
Head of Americas - Cullen International
Argentina

Omar de Leon Boccia
Executive Director - Teleconsult
Uruguay

Lilia Liu
Executive Director - Lilia Liu & Associates (LLASO)
Panama

Maryleana Méndez
Secretary General - Inter-American Association of Telecommunication Companies (ASIET)
Costa Rica

Oscar Messano
President - Centro de Capacitación en Alta Tecnología para Latinoamérica y el Caribe (CCAT LAT)
Argentina

César Moliné Rodríguez
Director of Cybersecurity - Electronic Commerce and Digital Signature
Dominical Institute of Telecommunications (INDOTEL)
Dominican Republic

Gonzalo Navarro
Executive Director - Latin America Internet Association (ALAI)
Uruguay

Rodrigo de la Parra
Vice President - Stakeholder Engagement & Managing Director - Latin America & Caribbean
The Internet Corporation for Assigned Names and Numbers (ICANN)
Mexico

Sissi de la Peña
Digital Commerce and International Organizations Manager
Latin America Internet Association (ALAI)
Mexico

Eric Ramírez
Director - Electronic Government
Government of El Salvador
El Salvador

Rodrigo Ramírez Pino
President - Chilean Chamber of Digital Infrastructure (IDICAM)
Chile

María Eunice Rivas Robleto
Executive Secretary - Nicaraguan Council of Science and Technology (CONICYT)
Nicaragua

Beatriz Rodríguez
President - Internet Society - Uruguay
Uruguay

Jorge Romo
Coordination of the National Digital Strategy (CEDN) - Office of President
Mexico

Eduardo Salido
Public Affairs and Policy Manager Latin America - Telefonica
Spain

Andrés Sastre
Regional Director - Inter-American Association of Telecommunication Enterprises (ASIET)
Uruguay

Thiago Luis Sombra
Partner - Mattos Filho - Veiga Filho e Marrey Jr Law Firm
Brazil

Paloma Szerman
Senior Regulatory Policy Manager LATAM - GSMA
Argentina

Fernanda Teixeira Souza Domingos
Federal Prosecutor - Federal Prosecution Service
Brazil

Berioska Torres
Under Secretary - Development of Information Society and e-Government
Ministry of Telecommunications and Information Society (MINTEL)
Ecuador

Paloma Villa Mateos
Public Policy Manager - Telefonica
Spain

Juan Manuel Wilches Duran
Telecommunications and Digital Transformation Consultant
Colombia

Cristina Zubillaga
Senior Consultant - Former Deputy Director
National Agency for e-Government and Information Society (AGESIC)
Uruguay

The Internet & Jurisdiction and ECLAC regional status report 2020 is the region's first comprehensive exercise to map the different policy trends revolving around the transboundary nature of the Internet and how it affects different stakeholders, such as governments, companies and civil society.

How might different regional and national regulations create barriers that hinder cross-border e-commerce and investment in digital markets? What economic and social benefits could be realized by harmonizing frameworks throughout the region?

A better understanding of this scenario is a key factor in fostering investor confidence, promoting innovation and economic diversification, attracting more confidence in the use of e-commerce and boosting a market of more than 600 million people, while opening up opportunities for businesses and particularly for small and medium-sized enterprises. Conversely, uncoordinated action by a wide range of actors and initiatives risks hampering the digitization of economies, governments and societies.

In order to help policymakers navigate the challenges ahead, the Internet & Jurisdiction Policy Network (I&J), in coordination with the United Nations Economic Commission for Latina America and the Caribbean (ECLAC), presents the key findings of the regional status report 2020.

Ahead of the launch of the full regional status report in late 2020, the key findings set forth here provide a robust snapshot of the upcoming report. They include a preliminary mapping of policy trends, thereby providing analysis of legislative developments in the region around the right to be forgotten, geolocation and smart agriculture, among other topics.

ECLAC

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

LC/TS.2020/68