IMSISS
International Master
Security, Intelligence
& Strategic Studies

Erasmus
Mundus

The role of Internet Service Providers in protecting digital rights

July 2022

2408232F

225122

15487759

Presented in partial fulfilment of the requirements for the Degree of International Master in Security, Intelligence and Strategic Studies

Word Count: 20, 067

Supervisor: Dr David Erkomaishvili

Date of Submission: 25/July/2022

University of Glasgow

DCU

UNIVERSITY OF TRENTO

CHARLES UNIVERSITY

Table of contents

Index of figures

Index of graphs

Index of tables

Index of maps

List of acronyms

ACS	Association of Caribbean States
ALADI	Latin American Integration Association (ALADI for its acronym in Spanish)
ALBA	Bolivarian Alliance for the Peoples of Our America (ALBA for its acronym in Spanish)
APC	Association for Progressive Communications
BEREC	Body of European Regulators for Electronic Communication
CAN	Andean Community (CAN for its acronym in Spanish)
CARICOM	Caribbean Community and Common Market (CARICOM for its acronym in Spanish)
CELAC	Community of Latin American and Caribbean States (CELAC for its acronym in Spanish)
CDA	Communications Decency Act (EEUU)
CIDA	Canadian International Development Agency (ACDI for its acronym in Spanish)
CJEU	Court of Justice of the European Union
DCM	Digital Millennium Copyright Act (EEUU)
DGA	Data Governance Act (EU)
DMA	Digital Markets Act (EU)
DPA	Data Protection Authority
DPI	Deep Packet Inspection
DSM	Digital Single Market
ECHR	European Convention on Human Rights
ECLAC	Economic Commission for Latin America and the Caribbean, (CEPAL for its acronym in Spanish)
ECtHR	European Court of Human Rights
EDRi	European Digital Rights
EDPB	European Data Protection Board

EDPS	European Data Protection Supervisor
ENISA	European Union Agency for Cybersecurity
ePR	ePrivacy Regulation (EU)
EU	European Union
EuroDIG	European Dialogue on Internet Governance
Europol	European Police Office
EU INTCEN	EU Intelligence and Situation Centre
FOIA	Freedom of Information Act (EU)
GDPR	General Data Protection Regulation
IANA	Internet Assigned Numbers Authority
IACHR	Inter-American Commission on Human Rights -OAS (CIDH for its acronym in Spanish)
IADB	Inter-American Development Bank (BID for its acronym in Spanish)
ICANN	Internet Corporation for Assigned Names and Numbers
IDB	Inter-American Development Bank
IDRC	International Development Research Centre (Canada)
IGF	Internet Governance Forum
ISP	Internet Service Providers
ITU	International Telecommunication Union
LACNIC	Internet Address Registry for Latin America and the Caribbean (LACNIC for its acronym in Spanish)
LIBE	Committee on Civil Liberties, Justice and Home Affairs (LIBE) (EU)
NetzDG	Network Enforcement Act - Germany (NetzDG for its acronym in German)
NRA	National Regulatory Authority
OAS	Organisation of American States (OEA for its acronym in Spanish)
OSCE	Organisation for Security and Co-operation in Europe

R3D	Network in Defence of Digital Rights
TSM	Telecommunications Single Market
UN	United Nations
W3C	World Wide Web Consortium
WCT	WIPO Copyright Treaty
WIPO	World Intellectual Property Organisation

Chapter 1. Introduction

Modern-day life is increasingly dependent on the internet and digital media. Across the globe, economic, commercial, political, cultural, and social activities rely heavily on the internet's operability. Consequently, internet governance and cybersecurity have emerged as significant concerns for various governments.

However, due to the internet's characteristics, such as deterritoriality, anonymity, and worldwide reach, regulating and protecting it has become a significant legal, technical, and political challenge.

In this respect, when discussing intermediaries' regulation, it is difficult to ignore its impact on digital rights, particularly when it comes to the Internet Services Providers (ISP) position in copyright defence or national security concerns.

Due to their unique nature, the role of internet intermediaries is becoming increasingly controversial. In the case of ISPs, it is critical to understand the breadth and complexity of their intervention in internet protection and governance. This situation raises two significant questions: When it comes to regulating and protecting cyberspace, whose interests are prioritised and what are the primary cybersecurity concerns?

Incorporating private players for their technological capabilities into (cyber) national security and copyright defence activities presents a considerable challenge. ISPs, for example, have evident private and for-profit interests. They are actors in the realm of the services market and are therefore unfamiliar with the responsibilities of carrying out security-related or policing functions. Furthermore, concepts such as transparency and accountability are foreign to them, just as their priorities differ from those of the states.

1.1. Objectives

Against this context, this study aims to investigate the role of ISPs in preserving digital rights. For that purpose, the European Union and the Organisation of American States are used as case studies since they are two significant worldwide players involved in digital governance and cybersecurity who are actively trying to reform practices and regulations in their respective areas of influence.

1.2. Research questions

The primary research question guiding this dissertation is: What is the role of Internet Service Providers in protecting digital rights in the European Union and the Organisation of American States? The secondary questions are *(i)* Which actors are, and how are they protecting digital rights in the EU and OAS? *(ii)* What freedoms are affected by regulatory gaps in EU and OAS? *(iii)* How is digital rights protection promoted in the EU and OAS?

1.3. Hypothesis

The central hypothesis holds that three critical factors determine the ISP's role in protecting digital rights: 1) deterritorialization of the state, which makes ISP's technological expertise indispensable, 2) new threats, unidentifiable and global in scope, which require a multistakeholder effort, and 3) anonymity, that leads to citizenship to yield freedoms in the name of (cyber) security to combat unknown actors.

The secondary hypothesis claims that:

- Human rights protection is no longer the exclusive task of the state. Today, in the EU and OEA’s context, the private sector

plays a key role in (cyber) security tasks, which raises controversy regarding transparency and accountability.

- The freedoms affected are privacy, access to information, and free speech. The citizenry also moves into a scenario with strict measures such as surveillance in the presence of identifiable threats.

- In the European Union and the Organisation of American States, digital rights protection takes a back seat to other concerns such as (cyber) national security and copyright protection.

1.4. Chapters overview

In order to test the hypotheses stated above, this study is structured as follows: The first chapter presents the objectives, research questions, and hypotheses. Additionally, it describes the theoretical and methodological instruments used for this research.

The second chapter discusses the current state of the art on the intermediaries and Internet Service Providers' role in (cyber) national security tasks, digital rights protection, and liability regimes, along with a bibliographic exercise with *Bibliometrix*.

The third chapter develops the theoretical and conceptual framework, examining propositions such as the social contract and its applicability in the digital realm, as well as Thomas Hobbes' conceptualisation of Leviathan. In addition, the state protagonist position vs market actors is examined using Susan Strange’s insights. Furthermore, Michael Foucault's notions of power and surveillance are reviewed in the context of digital security. The chapter concludes with a discussion of internet gatekeepers and net neutrality.

In the fourth chapter, the capabilities and constraints of ISPs in terms of internet governance are examined. Moreover, the chapter explores the substance of the Manila Principles.

Chapters 5 and 6 examine the cases of the European Union and the Organisation of American States, respectively. In particular, the chapters offer an overview of both actors, the type of ISP liability framework currently in force, and their limitations.

Chapter 7 develops a comparative analysis of previously mentioned contexts and describes the present situation of digital rights in each region. Finally, the conclusions reveal the most significant findings and test the proposed hypotheses.

1.5. Methodology

This dissertation is mainly based on a qualitative and comparative study. Additionally, as part of the theoretical framework, political and social science assumptions are examined in light of the digital context.

The case studies concentrate spatially on Europe and the Americas, focusing on the European Union and the Organisation of American States. The research includes descriptive and comparative analyses to illustrate the capabilities and constraints of Internet Service Providers in these regions.

The data sources include academic articles and books, as well as grey literature such as research reports, working papers, conference proceedings, white papers, policy documents, and reports produced by government agencies, academics, businesses, and industries belonging to regional and international political, economic, and telecommunications organisations. The time range spans from the first

legislative attempts to regulate online activities to the most recent debates in June and July 2022.

Chapter 2. State of the art and methodology

The current academic production on digital rights and cybersecurity is diverse. It focuses on the various elements and actors that make up the digital sphere. The topics include protecting critical infrastructure and confidential data, information warfare, fake news, online propaganda, misinformation, etc. Generally, a large body of literature is currently devoted to the diverse layers[1] that make up the cyber world. This variety exhibits the complexity of the digital space and its challenges in terms of security in all dimensions, including civil liberties protection.

As a result, the need for a multidisciplinary approach to face today's challenges has arisen. One of the most crucial elements for this task is, without a doubt, the involvement of the so-called intermediates. Their role has been analysed in the academic literature, emphasising its position in digital governance (LSE IDEAS, 2018; OECD, 2010; Carrapico & Farrand, 2017; Clemente, 2013, and Goldsmith & Wu, 2006) the importance of ISPs adopting sound security practices (Etzioni, 2014; Rowe et al., 2011, and Butler & Lachow, 2012), the critical relevance of their involvement in tackling cybercrime (Hiller & Russell, 2013; Levite et al., 2018; Hare, 2009, and Lachow, 2016) the pressing need for their collaboration with the state (Hiller & Russell, 2013; Harknett & Stever, 2009; Mee & Chandrasekhar, 2021; Carr, 2016; Etzioni, 2011, and Cavelty, 2015), and their contribution to the evolution of communication infrastructure (Buzatu, 2020).

Nevertheless, there is a paucity of research on their function in cybersecurity tasks and how it affects people's digital rights (Buzatu,

[1] The layers refer to the model proposed by Dr Martin Libicki that conceives cyberspace in four layers, 1) physical, composed of processors, routers, and other types of hardware, 2) syntactic, which encompasses programs that control systems functioning, 3) semantic, which compiles the information and 4) pragmatic, which is a layer that does not yet exist and, if it did, would deal with why a statement was made, or a message was delivered. Source: Libicki, (2007).

2020). Particularly noteworthy is the literature on copyright protection, which is extensive (Romero, 2006; Shushaanth & Prakash G, 2020; Mittal, 2004; Unni, 2001; Shalika, 2019; Weber, 2010; Wan, 2011; Chen, 2017; Paynter & Foreman, 2019; O'Sullivan, 2014; Mishra & Dutta, 2009; Skelton, 1998; Birchall, 2018, and De Beer & Clemmer, 2009) with some exceptions concerning freedom of expression (Malaja, 2014; European Parliament, 2018; Center for Democracy and Technology, 2012, and Article 19, 2013).

Based on the preceding, there is still considerable work to be done to understand the repercussions of the engagement of a non-state actor in digital governance and its implications for citizens' freedoms. Therefore, a *Bibliometrix* analysis was done to delve into the state-of-the-art in this field.

Bibliometrix is a library function in the statistical programming language R that allows users to perform bibliometric analysis. Through this function, three bibliographic searches were carried out in the *Scopus* database. *Scopus* was selected since —from all the databases in which *Bibliometrix* operates— it had the most results —number of articles— for the specified terms.

The following keyword combinations were used in the academic searches: "Internet Service Providers" in conjunction with "international security," "liability regimes," and "digital rights." The words were chosen to visualise literary production focusing not only on digital rights, for example, but also to discover how the topic is explored concerning the ISPs' participation.

The same analysis was carried out with the other keywords —International security and liability regimes— to analyse the state of academic study on the engagement of ISPs in international security

tasks and in establishing liability regimes. The term "International security" was selected because it produced superior outcomes compared to "national security".

The searches range from 1995 to 2022. The period frame corresponds to the signing of the World Intellectual Property Organisation's (WIPO) Copyright Treaty (WCT) in 1996. Since liability regimes have been primarily inspired to protect copyright online, it was considered a milestone date. The search was prolonged by one year (1995) to assess the impact of the WCT.

Three different types of analysis were performed: 1) yearly scientific production, which depicts in a graph the number of articles published through time on a particular topic, 2) a map showing the countries with the most articles on the subject, and 3) a visualisation of keywords used in publications correlated with publishing countries and authors' academic affiliations.

2.1. Scientific production on Internet Service Providers and international security

According to the findings of the initial search —Internet Service Providers and international security—, the following results were found:

General Information: 217 academic documents were identified, produced between 1995 and 2022.

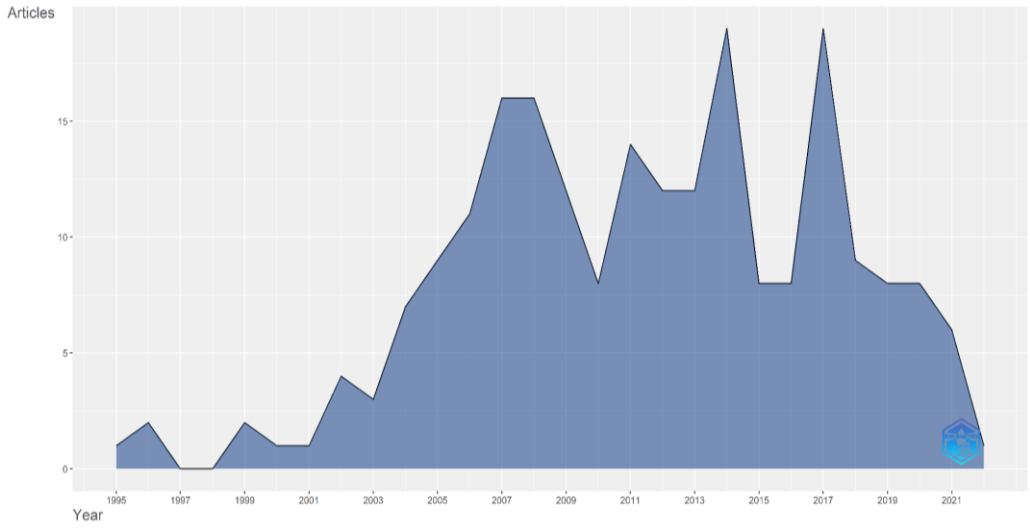
Annual academic production: From 2001 forward, there has been an increase in academic production. Overall, there have been periods of high output, but there have also been significant declines. It is worth noting the growth following 2001, which may be attributed to the entrance into effect of the World Intellectual Property Organisation's

(WIPO) Copyright Treaty (WCT) in 2002, one of the two most important international instruments in the field (WIPO, 2002).

The rises in 2014 and 2017 might also be attributed to the Compendium of United States Copyright Office Practices' release in those years (U.S. Copyright Office, 2017).

While it may be hard to link trends in favour of copyright protection to conventional international security concerns, there is no doubt that global economic security is intimately connected. Additionally, copyright protection is a contemporary issue that promotes international collaboration to safeguard diverse financial interests.

Graph 1. Annual academic production - Internet Service Providers and International security

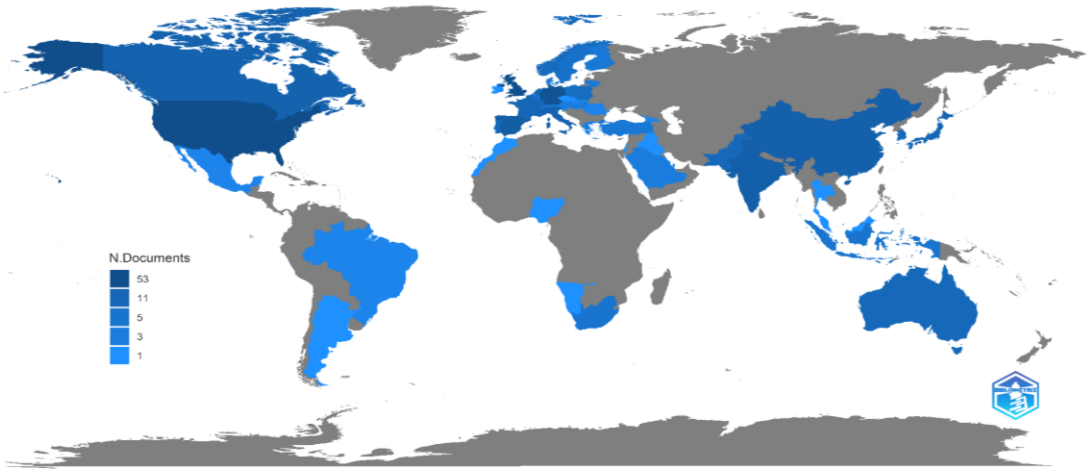


Source: Author's elaboration

Geographies of academic production: Map 1 depicts the countries with the highest levels of scientific productivity in this field, including the United States, the United Kingdom, Germany, Spain, India, and China. The concentration of literary production in particular nations might be attributed to government initiatives to achieve legal advances in this field, which encourages academic analyses. In this respect, the United States,

the United Kingdom, and Germany are considered leaders in copyright protection (GIPC, 2017). They are also the nations that concentrate the scholarly output in this area.

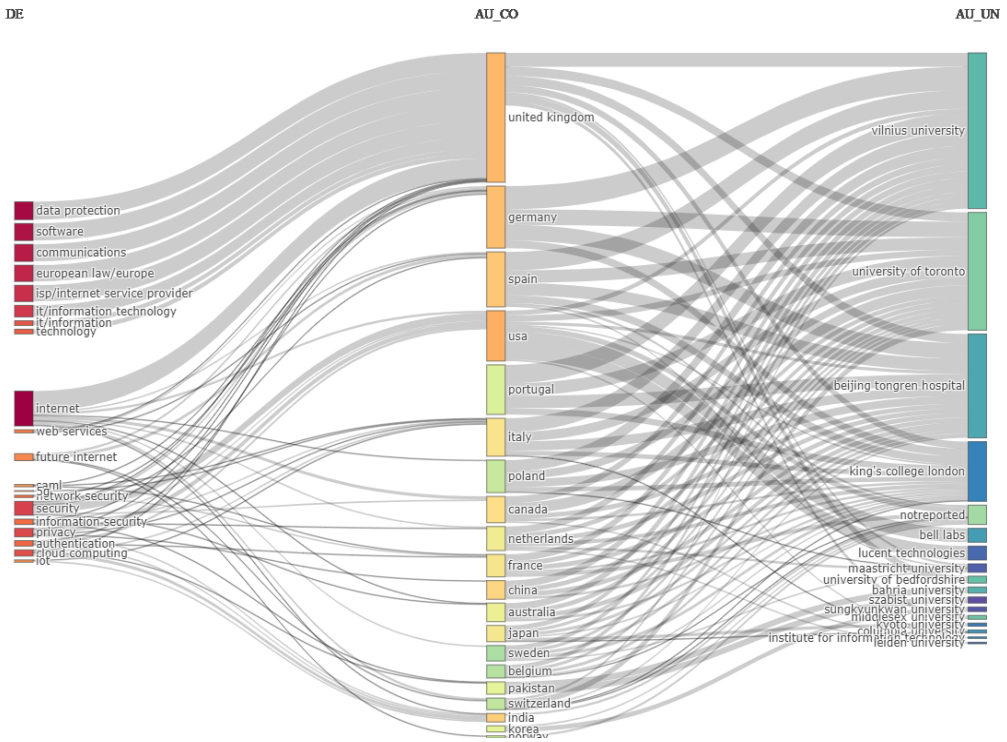
Map 1. Country scientific production - Internet Service Providers and International security



Source: Author's elaboration

Areas of interest by country and research institute: Figure 1 presents the keywords used in the collected publications, the location, and the authors' affiliation. As can be observed, keywords such as data protection, European legislation, and Internet Service Providers are relevant in the U.K. academia by scholars linked with various universities such as Vilnius University, the University of Toronto, and King's College London. Other terms, such as network security and privacy, interest scholars in the United States and Australia linked with diverse institutions. Finally, academics in Italy, for example, are interested in the Internet of Things, authentication, and information security. Important to note is that those scholars are connected with the University of Vilnius, the University of Toronto, and King's College London.

Figure 1. Correlation among keywords, location, and researcher affiliation - Internet Service Providers and International security



Source: Author's elaboration

2.2. Scientific production on Internet Service Providers and liability regimes

When it comes to ISPs and liability regimes, it has been discovered that

General Information: A total of 25 papers spanning 1998 to 2021 were collected.

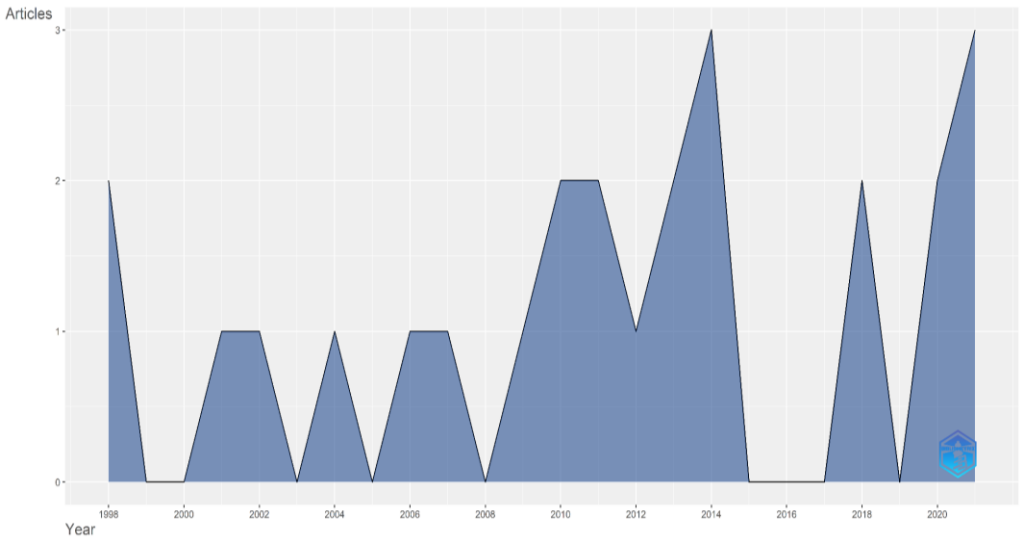
Annual academic production: Graph 2 depicts the yearly academic output of articles on ISPs and liability regimes. As the graph demonstrates, there are peaks and valleys, with significant rises in 2014 and 2020. The increase in 2014 might be attributed to the European Commission's submission of draft legislation on the European single market for electronic communications in 2013 (EPRS, 2014). The peak

might also result from events such as SFR's violation of French net neutrality laws by altering HTML content on the mobile internet in 2014 (Fiedler & McNamee, *n.d.*).

Regarding 2016, it can be noted that it was the year in which the European Commission started to issue yearly reports from National Regulatory Authorities (NRAs) on their compliance with open internet laws (European Commission, 2022a), which may have a marginal effect on academic productivity, but does not have a considerable impact. On the other hand, the rise in 2020 might result from a recent legislative session in the United States, during which 43 states and Guam addressed broadband in various areas (Morton, 2021).

The outlined legislative events may demonstrate correlation but not causation, as legislative activity continuously occurs throughout time. Nevertheless, certain events may catapult an issue onto the academic agenda.

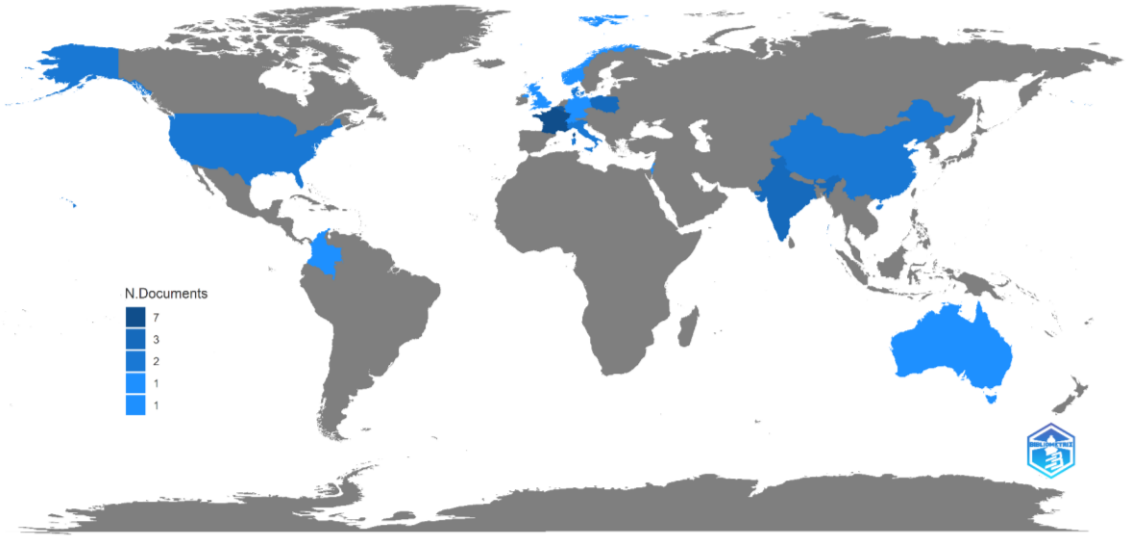
Graph 2. Annual academic production - Internet Service Providers and liability regimes



Source: Author's elaboration

Geographies of academic production: In terms of scientific production, as indicated in Map 2, France produces most of the scholarly articles, followed by Belgium and India. Here, it is crucial to recall that this statement should be considered cautiously, as the small sample analysed is not totally representative since it only includes articles from the *Scopus* database and not the total academic production. This restriction applies to the other two searches as well.

Map 2. Country scientific production - Internet Service Providers and liability regimes



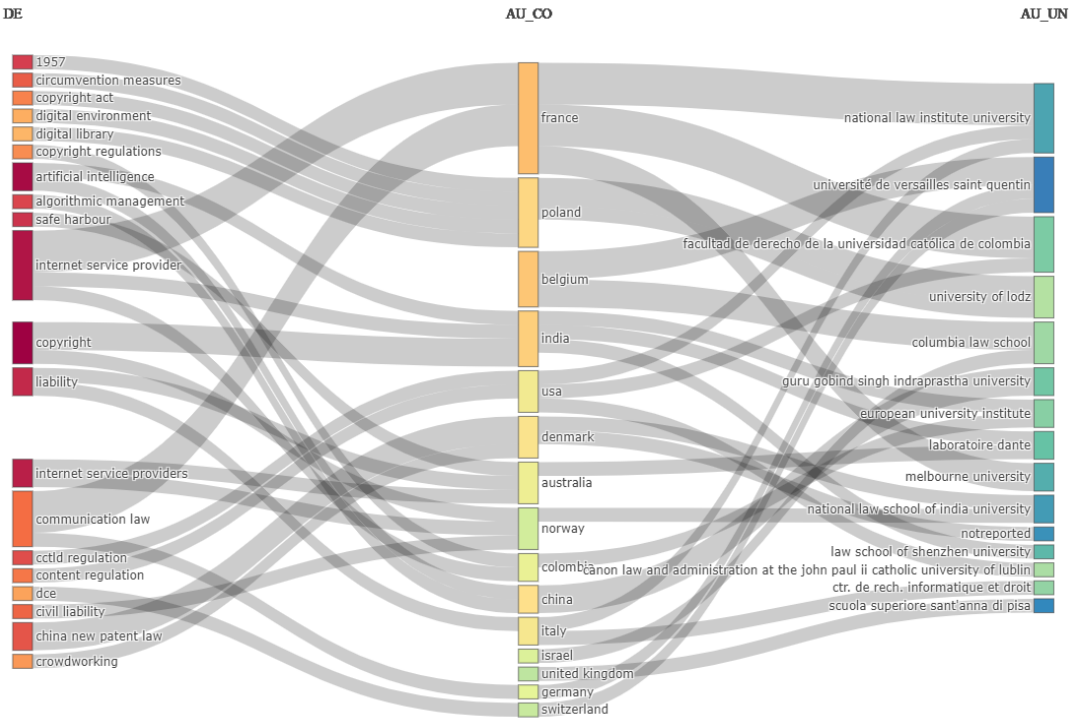
Source: Author's elaboration

Areas of interest by country and research institute: In terms of the correlation of keywords, geographical location, and affiliation, scholars located in France and connected with universities such as the National Law Institute University, the University of Colombia, and Melbourne University have a strong interest in ISP and communications laws.

Another significant trend is the growing interest in copyright and liability among scholars in India and connected with institutions such as the

European University Institute, Laboratoire Dante, and Shenzhen University.

Figure 2. Correlation among keywords, location, and researcher affiliation - Internet Service Providers and liability regime



Source: Author's elaboration

2.3. Scientific production on Internet Service Providers and digital rights

Finally, during the analysis of academic articles on Internet Service Providers and digital rights, the following findings were revealed:

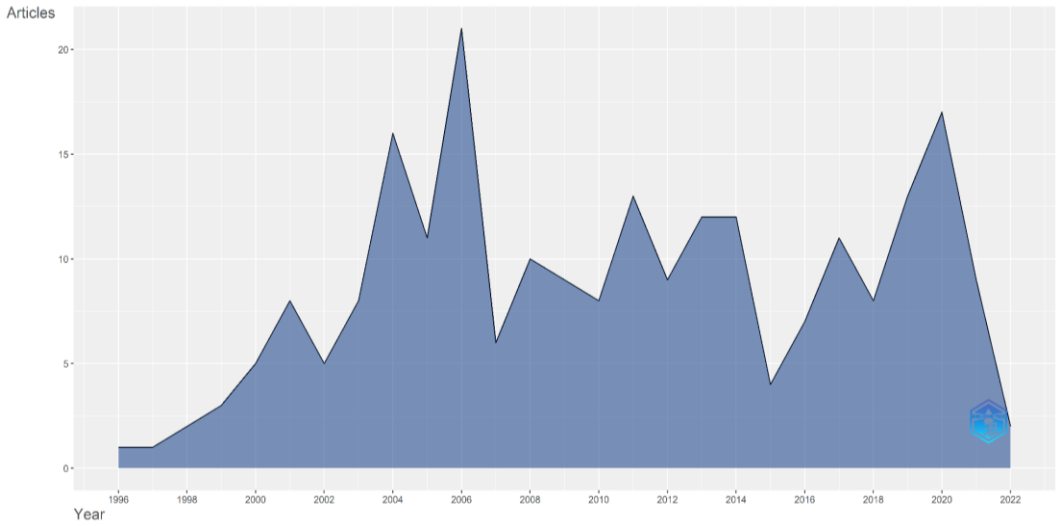
General Information: There were 231 documents retrieved that were published between 1996 and 2022.

Annual academic production: As Graph 3 indicates, scientific publications have increased significantly in recent years, particularly since 1996, with marked peaks in 2004, 2006, and 2020.

Concerning the political background that may have influenced the peaks, the Association for Progressive Communications (APC) established the APC Internet Rights Charter in 2001 (APC, 2006). Since then, efforts to promote and safeguard digital rights have expanded, and the charter was amended in 2006 (APC, 2006). Additionally, the UN Internet Governance Forum (IGF) has been tasked with interpreting and applying human rights on the internet since 2009, resulting in a substantial number of publications (United Nations, *n.d.*).

Adopting initiatives and establishing organisations devoted to protecting digital rights is a recent trend that may be correlated with the general increase in scientific activity.

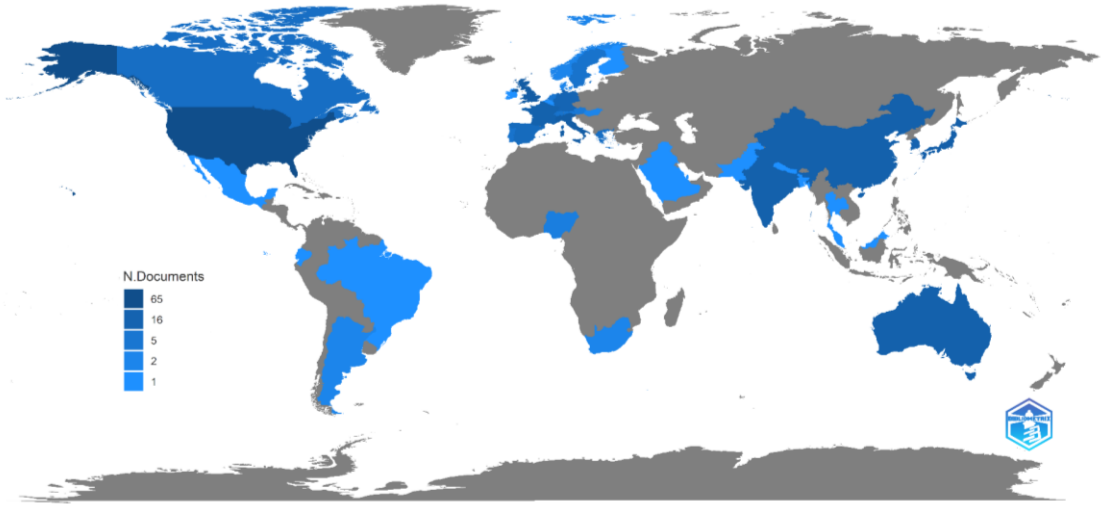
Graph 3. Annual academic production - Internet Service Providers and digital rights



Source: Author's elaboration

Geographies of academic production: Regarding the number of publications by nation, the United States is at the top of the list, followed by the United Kingdom, Italy, and Japan (see Map 3).

Map 3. Country scientific production - Internet Service Providers and digital rights



Source: Author's elaboration

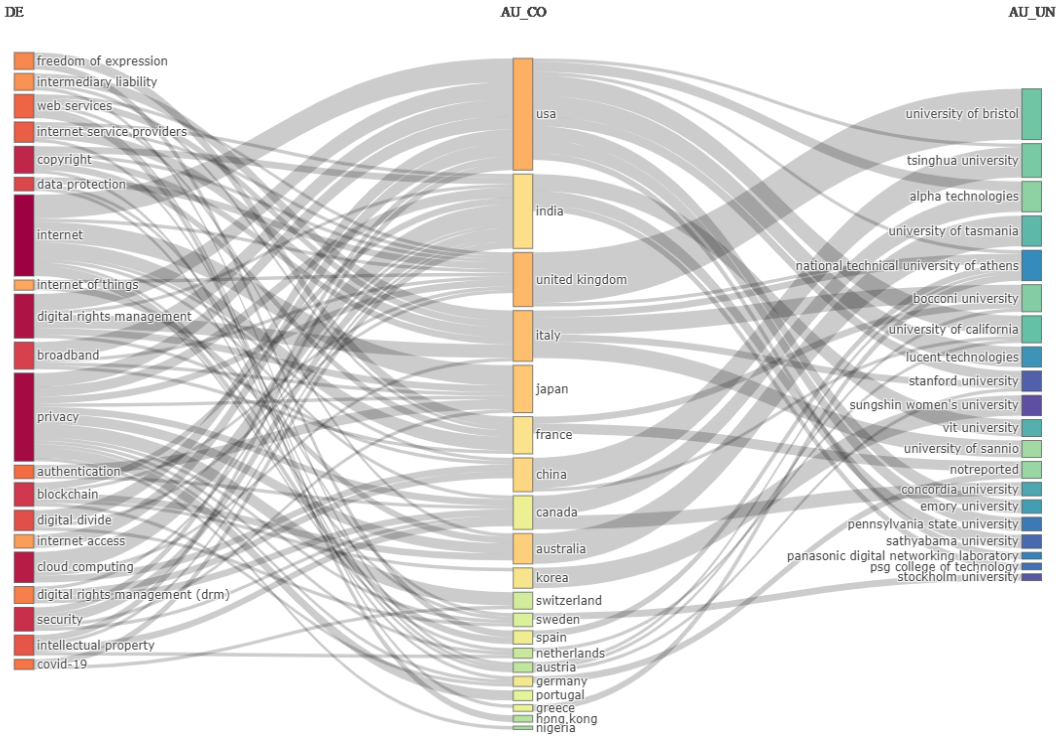
Areas of interest by country and research institute: In terms of the correlation between geographical location and academic affiliation, there is considerable research interest in the internet, digital rights management, privacy, the digital divide, and intellectual property among scientists based in the United States and affiliated with institutions such as Alpha Technologies (a telecommunication company), the University of California, Stanford University, and Pennsylvania State University, to name a few.

On the other side, researchers based in India and mostly affiliated with the Vellore Institute of Technology, Sathyabama University, and PSG College of Technology mainly focus on Internet Service Providers, copyright, cloud computing, and security.

Other researchers in the United Kingdom are interested in online services, data protection, copyright, privacy, and blockchain. It is important to note that they are mostly linked with the University of Bristol

and, to a lesser extent, the National Technical University of Athens (see Figure 3).

Figure 3. Correlation among keywords, location, and researcher affiliation - Internet Service Providers and digital rights



Source: Author's elaboration

2.4. State-of-the-art synthesis

As evidenced by the literature review and analysis conducted through *Bibliometrix*, most literary production may be classified into two broad categories: economic and political. Within the former, technical guideline evaluations on critical infrastructure protection and the associated costs have been published. Another influential topic is the collaboration between the finance industry, government, and ISPs to safeguard critical economic interests.

In the second category, the articles focus on the political dimension, highlighting analyses of specific proposals for regulating digital markets or copyright protection and those examining the outcome of negotiations, the approval of legislative amendments, or special sessions in parliaments on issues such as net neutrality.

The prevailing debate on international security and digital rights centres on economic security. In this view, digital rights are analysed in the context of proposals for copyright protection or net neutrality rather than in relation to national or international security tasks and their potential impact on digital rights.

In light of this, it is essential to broaden academic research on digital rights and delve deeper into how ISP involvement in digital governance can harm citizens' freedoms. For this purpose, the following section presents the theoretical-methodological frameworks that guide this dissertation and the geographical and temporal scope.

Chapter 3. Theoretical and conceptual framework

Much has been published about the challenges around internet governance and the most latent threats. It is also broadly acknowledged that traditional domains of state action are profoundly altered by the internet's inherent qualities, such as spatio-temporal fluidity, absence of central authority, anonymity, and uncertainty.

Consequently, governments have modified their instruments and procedures for administering justice and security to account for cyber activities. The above involves more than simply adapting the legislative framework. It entails restructuring the state-citizen relationship, including new players to provide security and regulate citizens' activities.

Given the above, it is necessary to assess the state of the social contract in the age of cyberthreats to determine the extent to which liberties are sacrificed in the pursuit of security and who is accountable for providing protection, especially regarding digital rights. To that aim, the emergence of a digital Leviathan, the role of market actors, and the exercise of power and surveillance, among other topics, are analysed in this section.

3.1. On a digital social contract

The notion of the social contract was promoted by philosophers such as Thomas Hobbes, John Locke, Jean-Jacques Rousseau, and Pierre-Joseph Proudhon during the 17th and 18th centuries (Cardelli et al., 2020).

According to these scholars, the guiding principle that contributed to the emergence of societies was the need for a social contract in which people in their natural state[2] entered into a voluntary agreement to cede

[2] It refers to the state or circumstances in which individuals existed prior to establishing an arrangement between them. Each philosopher considers a particular state of nature; for example, according to John Locke, persons in their natural condition are solidary and driven by the need for self-preservation. According to

freedoms such as the use of force. Under this new agreement, besides acquiring a monopoly on physical coercion, the counterpart is also responsible for protecting the life, liberty, and property of the governed (Locke, 2010).

In political science, the "social contract" concept is transcendental since it implies the basis for the ruler's legitimacy, whether by divine mandate or by the consent of the ruled. Each philosopher argued for a particular form of governance and defined the roles and boundaries of authority. For his part, Hobbes advocated the concept of absolute authority (the sovereign) to which individuals would submit out of fear and who would also wield absolute political power (Hobbes, 1997).

Re-examining the contract in the digital context is critical because individuals inhabit a new space where the possibility of war persists, and the environment's characteristics bring them tantalisingly close to the state of nature (Cardelli et al., 2020), i.e., there is an absence of a central authority, a constant threat to the welfare, but also to property (intellectual property, for example), to security, and various freedoms such as free speech, information, and privacy.

In this context, the social contract operates in a complex scenario due to the digital space liquidity,[3] its ongoing evolution, and the impossibility of governing and identifying all individuals who inhabit it. Experts like Liaropoulos (2020) believe that digital activity and the area in which it takes place constitute a new social structure.

Hobbes, individuals in their natural state are dominated by impulses such as pride and revenge; therefore, the contract is motivated by the fear of losing life, liberty, and possessions. Sources: Locke (2010) and Hobbes (1997).

[3] It also refers to Bauman's studies on modernity, in which he identified specific characteristics that define contemporary society and used the metaphor of "liquidity" to emphasise the transience and volatility of social interactions, which are exacerbated in large part by the use of emerging technologies that introduce uncertainty into people's lives (Rocca, 2008). In this context “liquidity” refers to the continuously changing digital environment.

In the light of the above, the Leviathan has acquired a series of new capacities and responsibilities. These new responsibilities require additional actors outside the usually analysed state-citizen binary to include commercial actors as well. Thus, in today's social contract, companies delivering various services, such as connectivity or hosting platforms, hold political transcendence.

Along these lines, the authority adapts and adopts the required procedures to accomplish three critical tasks (Loewe et al., 2021):

1. Protection - which entails collective defence and the provision of human and legal security.
2. Supply - of essential services, infrastructure, and economic possibilities.
3. Participation - of citizens in the process of decision-making.

The new complexities also encompass the nature of citizenship. On this point, specialists such as Cardelli et al. (2020) consider that the digital environment remains "feudal" in nature, given that people are not even perceived as digital "citizens" but as "users" and, therefore, it is difficult to talk about distinct and identifiable citizenship (Cardelli et al., 2020). Furthermore, the internet's structure is not guided by the democratic values of liberty, equality, and popular sovereignty (Cardelli et al., 2020).

3.2. The new face of Leviathan

The "Leviathan" is a creature in Hobbes' narrative that depicts the union of people’s wills that merge to form a whole. Leviathan also represents the greatest concentration of power, sovereignty, political authority, and physical coercion (Hobbes, 1997).

Since, according to Hobbesian reasoning, "man is a wolf to man" (Hobbes, 1997), it was necessary to develop a strong figure with authority to govern all wills and provide security and well-being. Although Hobbes referred to absolute sovereign power (i.e., a monarch), the concept of a governing body providing protection remains relevant today.

Cyberspace and cyber activities deviate from the traditional forms mentioned in Hobbesian texts, such as citizenship, the sovereign, the conventional exercise of authority, territory, and the threats that face humanity in its natural state (Liaropoulos, 2020). Nevertheless, specific characteristics remain, such as the ongoing threat from other actors and the demand for a security entity.

In Hobbesian thought, life, liberty, and properties are the primary goods to be preserved. Still, little is addressed regarding how this security would be accomplished. In both Hobbes' historical context and today's, the quest for security can cause collateral damage.

Because of the features outlined above, cyberspace's protective activities represent new possibilities for exercising authority beyond legitimate boundaries. To put this into perspective, consider the issue of digital surveillance (described in detail below) and the vast amount of data collected by states for security purposes (Liaropoulos, 2020). According to Da Silva (2022), the existence of a narrative that promotes a sense of perpetual vulnerability contributes to the normalisation of invasive activities such as surveillance through an overwhelming sense of urgency for protection.

Hence, the perception of vulnerability reinforces the urgency of a digital Leviathan. As a result, citizens' rights are restrained, and any violation of the authority-proposed standards is punished, which also involves, as

Da Silva (2022) points out, the exercise of power, in this case, cyberpower.

In this respect, Liaropoulos (2020) questions whether the state of digital interactions has led society and governments to re-evaluate the political and moral norms of behaviour that regulate the agreement between government and citizens? The answer could be that there is reassessment which has led to the adaptation of state action, where limits may or may not be transgressed. Given this possibility, an accountability mechanism is required to protect citizens from the digital Leviathans, which comprise more than just government entities.

Striking a balance between room for manoeuvre and boundaries is a significant difficulty that —Liaropoulos (2020) notes— involves a new social contract with individuals, authorities, and companies. Further, creating a digital social contract burdens the state to ensure market actors' actions do not threaten civil liberties and human rights (Liaropoulos, 2020).

3.3. Between the state and the market

Political power structures evolve throughout time, including, demoting, strengthening, and weakening diverse actors. Susan Strange, a British academic, was particularly interested in these structures, noting an increasing influence of the private sector on state affairs (Strange & Palan, 2015) (Strange, 1996). This new player benefited from technological advancements and the economy's transformation, having a parallel impact on political and social institutions. Strange also stated that this logic resulted in a "diffusion of authority beyond national governments" (Strange, 1996, p.14).

In her book *The retreat of the state* (1996), Susan also claimed that the existence of multinational corporations puts territorial authorities under

strain. Consequently, the increasing number of transnational actors displaces the state's power in their favour (Strange, 1996). However, it is critical to recognise that the state cannot be replaced, although it must accept market players inside the national power structures.

When Susan's propositions are applied to the digital arena, it becomes clear that transnational and domestic market actors indeed alter political and social structures. Today, Strange's analysis of the territorial control dilemma is exacerbated by the private sector's activity in the digital sphere. A complex situation that, —in addition to causing a structural transformation— is connected to the exercise of sovereignty, as numerous scholars have analysed (Sassen, 1999; Kostopoulos, 2021; Perritt, 1998; Pohle & Thiel, 2020; Wagner, 2013; Hathaway, 2014; Keller, 2019; Katz, 1997; Coyer & Higgott, 2020 and Marsili, 2019, among others).

Various experts have also dubbed this interference "cyber-exceptionalism" (Pohle & Thiel, 2020 and Da Silva, 2022). The term suggests that the digital domain needs different laws and regulations than those applied in the offline sphere and that much of the internet functionality hinders the exercise of state sovereignty.

Upon this matter, Marsili (2019) argues that conventional sovereignty appears to be losing significance considering the expanding capabilities of non-state entities such as technology companies and intermediaries. Quite a relevant notion in the light of facts such as these actors' ability to influence political life (Cambridge Analytica), establish their own economy (Facebook and its proposal to create its own currency), confront the state (Apple refusing to give information access to US security agencies), develop communications infrastructure (funding projects such as undersea cables in Africa), censor political actors on

platforms (Twitter vs Trump) participate in international negotiations (for example, in the General Data Protection Regulation), or even carry out defence tasks (the possibility to authorise the hack-back in the face of cyberattacks), etc. (Marsili, 2019; Babinet, 2018, and Forden, 2015).

Kostopoulos (2021) proposes that states should also have offices or ministries that deal with non-state relations. These new entities would deal with issues that arise with technology companies and the exercise of digital sovereignty (Kostopoulos, 2021). The proposal mentioned above suggests the emergence of a new political forum.

The political forum will undoubtedly include additional topics such as new forms of cooperation, shifts in the balance of power, the scope of collaboration among diverse actors, and changes in the nature of the state, as well as the transnationalisation of technological players' activities (Coyer & Higgott, 2020). The above creates a new landscape for international relations and diplomacy diametrically different from the long-prevailing Westphalian system (Kostopoulos, 2021).

Notwithstanding the preceding, the state continues to perceive itself as the dominant component of Leviathan on many levels, including the legislative (Kostopoulos, 2021). Nonetheless, the expanding capabilities of all digital participants require reconsidering concepts such as power, surveillance, and the status of digital rights in this ever-changing environment. Therefore, the next section will examine the relevance of Foucault's assertions on power and surveillance in the digital domain.

3.4. Power and surveillance vs digital rights

When discussing sovereignty, power, and security on the internet, it is impossible to avoid referencing Foucault's postulates on power and the panopticon. Numerous scholars have examined the exercise of power

online from sociological, political, and legal viewpoints (Naruse, 2018; Vijay Mukane, 2016; Boyle, 2007; McMullan, 2015, and Hadfield, 2017).

Looking at cyberspace through the lens of Foucault entails considering diverse variables, such as control narratives, the applicability of the panopticon online, the exercise and nature of digital power, as well as modes of punishment and surveillance (Naruse, 2018 and Vijay Mukane, 2016). Therefore, this section concentrates on two critical concepts: power and surveillance.

For several reasons, it is essential to assume that Foucault's ideas are partially valid in the digital context, as there are apparent restrictions to the notion of corporeality, an important element when talking about the panopticon and how power and punishment are exercised over bodies (Vijay Mukane, 2016, and Foucault, 2014). In cyberspace, there is no materiality —at least not in terms of interactions— yet identities, interests, and power relations exist.

Contrary to the contractualist logic in which the state concentrates all authority, Foucault considers that power cannot be held but exercised and is disseminated and exerted in various areas of daily life, as different as the agents who hold it (Foucault, 1994). Foucault deems that the circumstances in which it occurs are diverse, and therefore power is ever-changing (Foucault, 1994). When the argument is applied to the digital spectrum, it is evident that there are power relations in cyberspace that operate horizontally to the state, for example, those of intermediaries.

Cyber-power relations are complex, and players such as civil society, the media, and socio-digital platforms should be included in the dynamics alongside those who operate beyond the bounds of the law,

or as Foucault depicts it, outside the bounds of normalised behaviour, such as hackers.

In terms of surveillance, various studies analyse 1) whether, or not the internet is a panopticon, highlighting the concept's limitations in light of the panopticon's restrictive qualities or 2) how online monitoring, often known as "data-veillance," is essentially a form of social control (Vijay Mukane, 2016; McMullan, 2015; Boyle, 2007; Brignall, 1998; Martin, 2013, and Stoycheff et al., 2019).

In this sense, it is possible to affirm that on the internet, dynamics of social control do indeed exist and involve not just states. Although in the panopticon, the prisoner does not know whether he/she is being observed, and the prisoner is a docile body, there is no doubt about the capabilities of intelligence agencies, tech companies and hackers in the post-Snowden era.

Additionally, as Vijay Mukane (2016) argues, the network inhabitants are not docile but active users, who in turn are also capable of occupying a place within power relations. In brief, the internet panopticon functions as a vigilante capable of monitoring online activities, and this vigilante requires market players to conduct this surveillance.

For its part, the observed prisoner stems from the measures he/she lacks (at the moment) to defend him/herself from this surveillance and to leave this condition because, as Foucault points out, individuals are also capable of exercising power and being more than they are (Foucault, 1994).

Another point worth emphasising is the development of punishment through time. In *Surveillance and Punishment* (2014), Foucault argues that one of the driving reasons behind the evolution of discipline forms is the growth of production and wealth, which manifests itself in the severity

of penalties for economic crimes. In the digital spectrum, it is possible to note the rise of discussions regarding copyright or industrial digital espionage and the centrality of this debate compared with other topics such as the exercise and defence of digital rights.

Bodies, —says Foucault— are traversed by power relations (Foucault, 2014). In this respect, on the internet, instead of bodies, it is possible to talk about ways of being and existing online and how these are also crossed by digital power.

3.5. The Gatekeeping's role

The unique function of ISPs in internet governance is the gatekeeper. In other words, they are responsible for managing access. Barzilai Nahon's Network Gatekeeper Theory (NGT) explains this social and technical function. According to the NGT, intermediaries exercise their regulating or controlling powers at the digital gates through which information transits (Laidlaw, 2012).

The gatekeeper's activities include selecting, aggregating, retaining, monitoring, channelling, shaping, manipulating, replaying, timing, locating, integrating, disregarding, and deleting information (Barzilai-Nahon, 2006). Following Barzilai Nahon's (2006) propositions, the gatekeeper is an entity that exercises authority via network-based mechanisms. These entities possess censorship, editorial, channelling, security, location, infrastructure, and regulatory powers (Barzilai-Nahon, 2006).

In their research, Barzilai-Nahon and Neumann (2005) also pinpoint the gatekeeper's nature as a political actor. Laidlaw (2012), on her part, emphasises the ability of these players to modify the behaviour of third parties when the state cannot do so, which is why governments turn to them to regulate behaviour in the digital world, a process known as

"decentralised regulation" (Cortés Castillo, 2017). Finally, the extent of the gatekeeper's duty might range from a bouncer (limiting admission and identifying who has or does not have access) to a chaperone (monitoring and influencing user behaviour) (Cortés Castillo, 2017).

As is already perceptible, ISPs, as gatekeepers, impact user behaviour by regulating access to information and defining what content is or is not lawful through the powers granted by liability regimes.

The state grants these surveillance and punishment capabilities through decentralised regulation of the copyright or national security tasks. It is a fact that the parameters under which gatekeepers' function substantially impact users' freedoms, reinforcing the control narratives, as referred to by Foucault's arguments.

Gatekeepers, however, must also adhere to certain principles, one of which is net neutrality. Net neutrality is regarded as the basis for exercising digital rights and is discussed in detail in the next section (Court of Justice of the European Union, 2020).

3.6. On Net Neutrality

Net neutrality is the principle that all online content should be treated equally. Net neutrality promotes access to apps, or online content should not be blocked, impeded, or delayed, and that content providers should compete on a fair playing field (Márquez, 2018).

Tim Wu, a professor at Columbia University, coined the term in the context of early discussions in the United States on data traffic control and the quality of internet services (Márquez, 2018). In his postulates, Wu refers to net neutrality as a user right that enables unlimited access to the network (Califano, 2013).

As for its current status, Berners Lee —widely regarded as the founder of the World Wide Web—, asserts that threats to neutrality have emerged significantly in recent years (Márquez, 2018).

Since its inception, the notion of net neutrality has argued for four freedoms: 1) to connect devices, 2) to run apps, 3) to run content packages, and 4) to get relevant information (Marsden, 2012).

In broad terms, it can be stated that there are two perspectives within the net neutrality debate: the first is to regulate the principle, as failing to do so would impact rights such as freedom of expression. The second encompasses the opposition to regulation since it would negatively influence investment and create barriers to innovation and reinvestment; this group primarily comprises the private sector (Márquez, 2018).

The net neutrality concept has several consequences for the exercise of individuals' freedoms since the imposition of accessibility limits based on the type of content or service to be accessed would impact rights such as privacy and access to information (Fiedler & McNamee, n.d.).

Nowadays, net neutrality is a topic on various nations' legislative agendas. It involves governmental and private sector players whose decisions will significantly impact the exercise of online freedoms.

Net neutrality, effective ISP regulation, and digital rights protection are components that continually interact with others, such as copyright protection, cybercrime prevention, and national (cyber) security. Balancing these interests will need ongoing legislative analysis; otherwise, cyberspace would be securitised in the name of economic interests, to name but one. It is therefore imperative to explore positive security concepts and the possibility of people-centred security in cyberspace.

3.7. People-centred security for cyberspace

This chapter analysed the emergence of social ordering and power distribution for governance and security supply on the internet. As discussed above, both ideas and practices have evolved over time. In general terms, there has been a change in how authority is exerted from a vertical hierarchy, with power concentrated at the top and exercised through state agencies/institutions, to a horizontal structure, less centralised playing field, and a redistributed power.

Following on, Susan Strange's ideas help examine those other players acting horizontally to the state who have gained significance and capabilities due to the technology revolution and globalisation process. These players transform the Leviathan's visage into a dispersed entity since governments need these participants to exert authority and control.

This dynamic implies new power relations and surveillance methods, in which telecommunications companies hold unique technical skills critical to maintaining peace and order in the digital sphere. However, such abilities also involve the user's vulnerability and the possibility of them being included in an online panopticon.

Under these conditions, policies and processes are required to monitor the Leviathans and guarantee that cybersecurity tasks do not infringe on governed liberties. Likewise, it is imperative to delimit and supervise the gatekeeper's functions and preserve net neutrality.

For this purpose, it is worth debating whether a state-centric approach to cyber security —which prioritises national security and economic interest— is the only possibility in the digital sphere.

The above calls for advocating a people-centred cybersecurity concept inspired by the UN proposals for "an approach to help [...] identify and

address the pervasive and cross-cutting challenges to the survival, livelihoods and dignity of [...] people" (United Nations, 2012). By emphasising the preservation of people's dignity, it is feasible to promote a citizen-centred and positive notion of cybersecurity that prioritises the defence of digital rights.

It is a matter of rebalancing the scale and no longer seeing the reflection on digital rights on the margins and in the shadow of existing arguments about digital governance and security. A debate in which, nowadays, national and economic interests seem to prevail over human rights ones.

Chapter 4. Private sector: Internet Service Providers

Although internet usage is common nowadays, little is known about its operation. Understanding the network's intricate dynamics is restricted to technical circles, while policymakers, legislators, and civil society are mostly unaware of its primary characteristics. This lack of knowledge permits legal gaps that establish uneven responsibilities and restrict the users' liberties.

The condition described above persists when dealing with several concerns. Among them are the ISPs' role in preserving copyright, combatting child pornography, defamation, and cybercrime. Although these concerns require immediate attention, they place intermediaries in a difficult position. ISPs are under pressure to learn new competencies, assume new obligations, and even be held liable for the acts of third parties. All the aforementioned exceeds their commercial interests and capabilities.

Therefore, it is essential to acknowledge the need for balanced tasks and policy frameworks that do not solely assign policing duties. Moreover, measures are required to protect the fundamental rights of internet users (Article 19, 2018).

Especially in national security and copyright, intermediaries should not be assigned surveillance or monitoring activities or be obliged to provide unlimited and unsupervised access to users’ data. It must be avoided to delegate responsibilities surpassing their competence or contradicting their core goal: delivering services and making profits.

In this context, it is critical to understand what so-called intermediates are, how they work, and their position on digital rights.

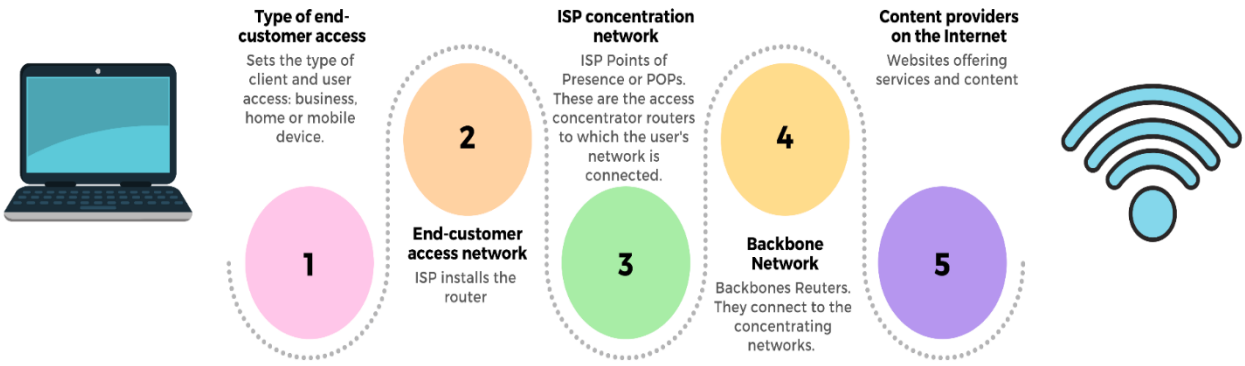
The Internet Service Providers are the mediators between the network and its users, allowing the latter to connect to the internet. In general

terms, "intermediary" refers to the services, equipment, and devices that enable internet access (Coyer & Higgott, 2020). Nevertheless, "intermediary" can also refer to firms whose services include web servers, social media platforms, and search engines (OECD, 2010 and Manila Principles on Intermediary Liability, 2015), each of which has unique capabilities and roles; therefore, the term must be clarified to avoid confusion.

For the purposes of this analysis, the OECD's definition is used: "internet intermediaries [are those who] bring together or facilitate transactions between third parties on the internet. They give access to, host, transmit and index content, products and services originated by third parties on the internet or provide internet-based services to third parties" (OECD, 2010, p. 20).

The user-to-global connection process consists of several layers, including several types of networks that make the ultimate connection feasible (see Figure 4). ISPs are split into three tiers based on their geographic reach, users, technology, and services. Tier 1 has the highest closeness (small geographic units), whereas tier 2 has national or regional scope, and tier 3 has a worldwide reach (Lopez, 2021).

Figure 4. ISP layers of service for internet connectivity



Source: Author's elaboration with data from Lopez (2021).

Intermediaries are so crucial in powering the digital era that it is estimated that 25 ISPs account for 80% of all digital traffic content (Hathaway & Savage, 2012). These companies, such as Vodafone, AT&T, BT, T-Mobile, Movistar, and Orange, to name a few (Hathaway & Savage, 2012), are now tasked not only with becoming internet gatekeepers and being held accountable by the judiciary for violations committed through their services but also with carrying out national security enforcement tasks.

4.1. Technical and legal capacities

As aforementioned, ISPs are the companies that provide access to the internet. In general, these players are telephone companies who, for a monthly charge, provide connection services and other services such as domain name registration and hosting (Master Internet and Computer, 2015). Furthermore, their reach can be national or international — relevant issue when referring to national jurisdictions (Master Internet and Computer, 2015).

When discussing security and protection tasks (for instance, regarding copyright), it is possible to divide ISP capabilities into two categories: 1) immediate actions, such as monitoring and removal of illicit content, and 2) long-term actions, such as the collection of digital evidence for judicial investigations (see table 1) (Tosza, 2021).

Table 1. Action modalities of ISPs in the reinforcement of national security tasks

Modality	Action
Immediate	Monitoring and removal of illicit content
Long-term	Data collection and cooperation in judicial investigations

Source: Author's elaboration with data from Tosza (2021)

Internet traffic monitoring can be accomplished by a technique known as Deep Packet Inspection, which is commonly used without the user's awareness (Cortés, 2012). Such methods allow the ISP to detect unencrypted content packets and divert or stop internet traffic (Barnett, 2019).

In the past, when ISPs transported "packets" of information, they could only view the "header" and not the full content of the communications. Today, with DPI techniques, ISPs may "open" and access the messages' content in real-time. DPI grants ISP more authority and precision. As a result of these new capabilities, ISPs can, —in addition to censoring or blocking content—, sort the processing of data packets to give different connection speeds, which is generally objected to since it would violate net neutrality (Riley & Scott, 2009).

Regarding ISPs' legal duties, they differ by regional regulations and country jurisdiction. Their collaboration with national authorities in countering illegal operations occurs under different modalities, including co-regulation, self-regulation, private regulation or enforcement (Tosza, 2021, and Hong & Li, 2011). Moreover, in the circumstances with no legislative framework, issues are settled case-by-case using the available legal tools (Bayer et al., 2007). The challenges arise when:

1. There are no clear liability statutes.
2. ISPs are granted excessive authority over users' activity.
3. They are granted surveillance and content removal capabilities, including storing information about users, keeping records of searches and internet browsing (Bayer et al., 2007).

Currently, there are several rules applicable to ISPs and vary significantly, for example, between those applicable in the United States and those in Europe, which is problematic when digital activities or the

reach of ISPs are transnational. The previously mentioned gatekeeper theory guides the design and adoption of legal frameworks in diverse circumstances (Cortés Castillo, 2017).

In this sense, gatekeepers have three modes of intervention: the first is to delimit the user's activities within the gatekeeper's domain, the second is to protect this domain so that external agents cannot intervene, and the third is to maintain order within the user-occupied area Cortés Castillo (2017).

In terms of enforcement, there are several dimensions of liability and immunity. For instance, in the United States, the Communications Decency Act (CDA) established an incentive for ISPs to work together to prevent undesired internet behaviours (Cortés Castillo, 2017). However, intermediaries were required to implement surveillance and monitoring procedures to comply with regulations, which was considered unreasonable (Cortés Castillo, 2017).

In response, Section 230 total immunity was preserved, under which ISPs are seen as an information-carrying medium and are not regarded as authors or liable for online content (Cortés Castillo, 2017). In particular, section 230 (c)(1) of the CDA states: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider" (Kelly, n.d.).

Similarly, "conditional immunity" is typically associated with copyright protection. The objective is to offer ISPs "safe harbours," i.e., ways or alternatives to avoid liability. In the case of the United States, the US Digital Millennium Copyright Act (DMC) stipulates a series of conditions,[4]

[4] Such as acting upon becoming aware of illegal activities.

if met, absolve the ISP of liability and, consequently, of the duty to policing (Cortés Castillo, 2017).

In terms of "subjective liability", ISPs are not responsible for applying specific laws but are accountable for following general ones and principles of civil liability (Cortés Castillo, 2017).

As can be seen, ISPs play an extremely vital role in maintaining order and enforcing internet rules. However, they are actors who require checks and balances to ensure that their activities do not stray from legality (Coyer & Higgott, 2020).

The excessive burden of liability is considered to be a "networked authoritarianism" in which major telecommunications companies are the extension of state authority, therefore, requiring transparency and accountability procedures (Coyer & Higgott, 2020) MacKinnon (2013).

Along these lines, various stakeholders have advocated several responsibilities that ISPs should embrace to protect users' rights while implementing laws; among these are: *i)* provide a reliable and accessible conduit for traffic and services, *ii)* provide authentic and authoritative routing information, *iii)* to provide authentic and authoritative naming information, *iv)* to report anonymised security incident statistics to the public, *v)* to educate customers about threats, among others (Hathaway & Savage, 2012).

In addition to enforcing regulations, ISPs are tasked with combating terrorism and cooperating with criminal investigations by sharing digital data (Tosza, 2021).These activities present a variety of obstacles — analysed in the next section— relating to technical capacities, human rights training, transparency and accountability systems, among others.

4.2. Limitations and challenges

Since ISPs are crucial to preserving the digital rule of law, it is paramount to consider the most pressing obstacles in the coming years. These include the technical and economic capabilities of ISPs to carry out their assigned responsibilities, the establishment of accountability mechanisms, capacity building and digital rights protection, as well as the importance of a cross-sectoral dialogue on their involvement in national security tasks.

In terms of **technical capacities**, given the volume of data that circulates daily on the network, it is exceptionally costly for ISPs to conduct monitoring tasks without incurring excessive costs that would render their business unsustainable (Cortés Castillo, 2017). Alternatives include using automatic filters to minimise expenses.

On this point, the European Union has advised adopting "safeguards" such as human verification of identified material when using this kind of filter (Vranckaert, 2020). However, the employment of automated tools remains a matter of discussion in the political and legal spheres since it would leave something as vital as freedom of speech in the hands of automated programmes.

Geography and the diverse regulatory systems applicable to global communications are also significant constraints. In this vein, what is considered unlawful differs from country to country, complicating ISP's work (Tosza, 2021). Moreover, even though nations may have implemented "safeguards" to protect individuals under investigation, their rights, and due process, cases frequently include servers located in countries with varying regulations.

The challenges for ISPs also involve **accountability and transparency mechanisms**. Since, in the face of increasing pressure from the

government and the private sector, ISPs could simply remove and block content to avoid sanctions, which would violate diverse rights (Article 19, 2018).

Article 19 (2018) has stated that the increased control of ISPs over online material may indicate that the state is outsourcing its censorship capabilities to third parties. For this reason, Article 19 (2018) recommends extending transparency to the decision-making process when removing or blocking content, as well as establishing and clarifying —through public statements— ISP's human rights responsibilities and commitments.

It is important to note that several civil society organisations are not opposed to the participation of the private sector in national security and public security tasks. What concerns them is the potential for abuse of power by intelligence agencies or arbitrariness on the part of the private sector. Civil society organisations, therefore, demand that any decision to take down content should be made with judicial intervention and that ISPs publicly report on requests for information by government authorities.

However, if internet service providers engage with human rights, they must first understand what this entails, i.e., how human rights and national legal frameworks are interpreted and applied. Similarly, ISPs must be aware of the legal tools available to defend themselves in cases where authorities expect cooperation beyond their capabilities. Naturally, this legal understanding extends beyond their traditional field of operation.

Another challenge involves **establishing a multi-sectoral dialogue** that includes actors from the private sector, ISPs, government representatives, regional actors, non-governmental organisations, and

civil society when developing liability regimes since there are several interests at risk, which must be balanced. So far, the discussion processes have lacked more robust engagement from non-governmental organisations, civic society, and ISPs.

Experts such as Tosza (2021) note that contemporary regimes tend to adopt a "responsibilisation" approach, where ISPs are compelled to judge regarding what is lawful and what is not and take action. The above is a serious concern, and several international organisations addressed it by proposing the Manila Principles in 2015 (CELE, n.d.). The Manila Principles aim to guide decision-makers when attempting to create and implement laws regarding intermediaries' liability and to consider the impact on human rights (CELE, n.d.).

4.3. Manila Principles and liability regimes

In March 2015, in the context of the RightsCon conference, a group of civil society organisations submitted the Manila Principles to aid legislators in developing liability regimes and protecting human rights (CELE, n.d.). The fundamental tenet of this proposal is that no intermediary should be held accountable for user content where ISPs are not engaged in authorising or modifying information (Morachimo, 2015).

One of the most significant contributions is that it places transparency and accountability at the centre of liability regimes. The principles consider it necessary for governments and ISPs to publish and regularly report on content removal rules (Morachimo, 2015).

The document is based on international instruments, including regional and international human rights standards and recommendations by the UN Special Rapporteur for Freedom of Opinion and Expression

(Electronic Frontier Foundation et al., 2015). The proposed principles include

1. Intermediaries should be shielded by law from liability for third-party content.
2. Order and requests for the restriction of content should be clear and unambiguous.
3. Content restriction policies and practices must be procedurally fair.
4. The extent of content restriction must be minimised.
5. Transparency and accountability should be built into content restriction practices.
6. The development of intermediary liability policies should be participatory and inclusive (Electronic Frontier Foundation et al., 2015).

Most notably, the document signatories acknowledge that the availability of technological methods to prohibit access to material does not qualify ISPs to judge its legality, as such powers should belong to an independent judicial authority (Electronic Frontier Foundation et al., 2015).

The principles also focus on the notice and notice system, which may apply to non-serious criminal cases. In addition, several concerns are promoted, such as procedural safeguards that should be included in the "safe harbour" mechanism, consistent with human rights standards (Electronic Frontier Foundation et al., 2015).

The proposal is significant because it protects users' rights, acknowledges the necessity for ISPs to collaborate with state authorities in criminal prosecutions, and supports the notion that ISPs should not be burdened with tasks that exceed their capacities.

It should be stressed that notwithstanding the apparent obstacles online content regulation faces, the state remains accountable for upholding human rights online. Such obligations are outlined not only in national and regional treaties on human rights protection but also in the *Tallinn Manual,* the most comprehensive legal document on international law for cyberspace.

In its section "International Human Rights Law," rule 36, "Obligations to respect and protect international human rights", refers to the responsibility of governments to protect individuals against infringements by third parties, such as ISPs (Schmitt, 2017).

Consequently, while ISP assistance is urgently required in law enforcement, the state has responsibilities regarding protecting human rights and due process. As mentioned in this section, the gatekeeper role subjects ISPs to excessive governmental pressure and allows for the potential of arbitrary judgments that undermine the user's liberties.

There is a need to develop balanced, fair, and transparent regimes at the national, regional, and international levels. Therefore, the following sections address the cases of the European Union and the Organisation of American States to assess the liability regime’s condition in both regions and the ongoing threats to digital rights.

Chapter 5. The European Union case

5.1. Background

Internationally, the European Union stands out for its ongoing attempts to regulate the vast array of internet-based activities. Several discussions have been undertaken to propose, amend, and expand legislative instruments for internet governance, defending intellectual property, protecting critical infrastructure, fighting against digital crime, and safeguarding personal data, among other concerns.

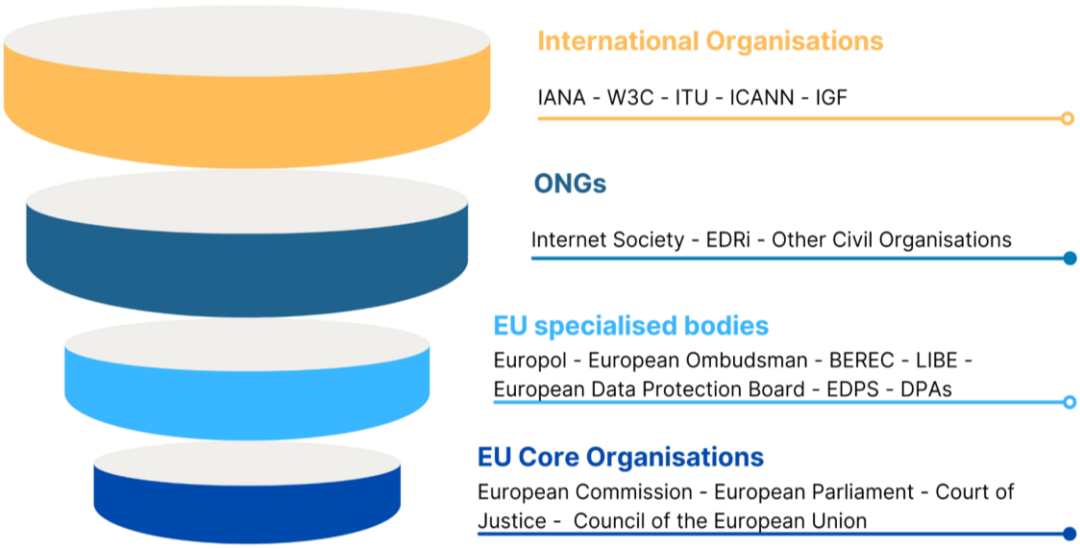
The European Union has played a leading role on the worldwide scale, beginning with its prominent participation in ICANN's reform (Internet Corporation for Assigned Names and Numbers), the transition to IANA (Internet Assigned Numbers Authority), and subsequently through its participation via the European Commission in the Board's discussions (Christou & Simpson, 2011).

Furthermore, the Council of Europe engages actively in the Internet Governance Forum and has released a series of announcements on digital governance (European Commission, 2014). Since Edward Snowden's 2013 revelations about worldwide monitoring by US intelligence agencies, the European Union and other countries have prioritised personal data protection and defining the boundaries and duties of all players engaged in providing digital services, including collecting, storing, and processing personal data (Morin-Desailly, 2014).

The European Union also began strengthening legal frameworks and organisations to prioritise data protection. From *Directive 2006/24 on the retention of data generated or processed* to the *Digital Markets Act* (DMA), several legislative instruments seek to establish a balanced ecosystem in which all actors perform tasks to preserve the internet's functionality and protect both providers and consumers (Karsten, 2013).

The European Union's institutional ecology concerning internet governance and digital rights protection includes the European Parliament (legislative, supervisory, and budgetary functions), the Council of the European Union (political guidance), the European Commission (legislative reinforcement), and the Court of Justice (justice administration) among other actors such as the European Ombudsman, the European Data Protection Supervisor, EDRi, Body of European Regulators for Electronic Communications (BEREC), and the European Data Protection Board (Adtran, 2021) (see Figure 5).

Figure 5. Institutional Ecology (EU) - Organisations active in internet governance and digital rights protection



Source: Author's elaboration with data from Adtran (2021)

Figure 5 depicts the players involved in European Union internet regulation, particularly personal data protection and digital rights. The regional digital ecosystem is the outcome of a continuous analytical and evolutionary process that keeps the European Union abreast of technological innovations.

In terms of digital rights protected by the EU, it is critical to highlight the right to privacy, freedom of communication, and freedom of information, which are a priority within recent legislative debates, particularly regarding net neutrality. The EU considers net neutrality a critical component since it reflects how rights are inextricably linked to their organisational and material dimensions (Court of Justice of the European Union, 2020). Therefore, supporting net neutrality entails keeping the conditions by which other rights may be exercised.

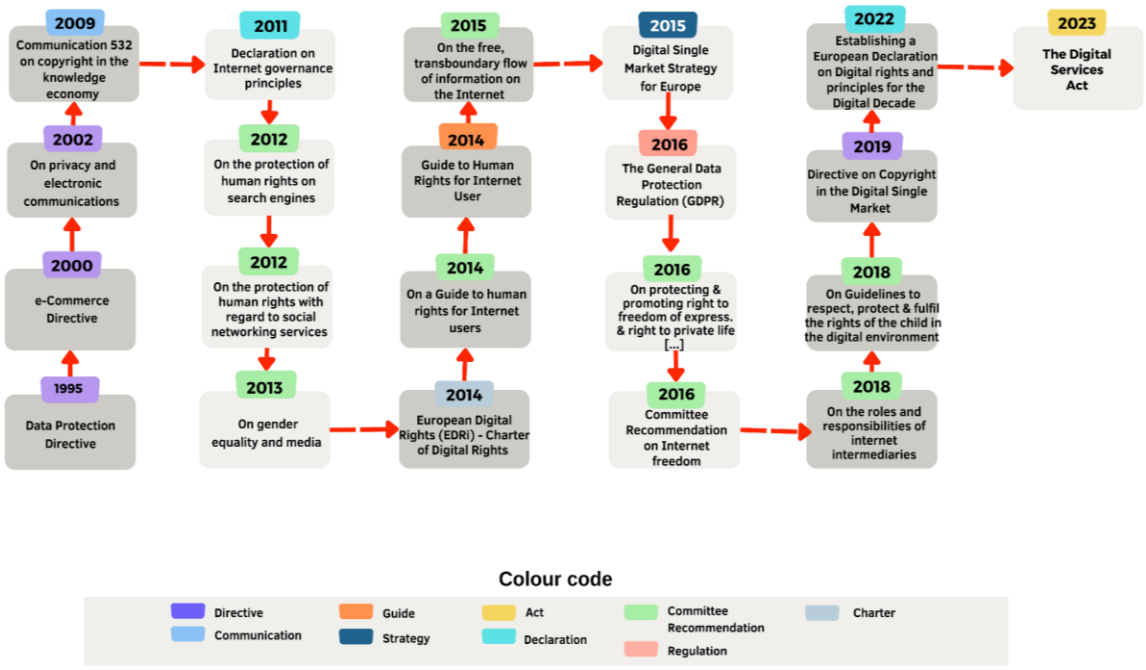
5.2. Type of liability regime

The existing ISP liability framework in the EU results from several resolutions and legal amendments concerning how the internet is administered, how digital rights are safeguarded, and who is accountable for what in the European digital realm.

In this sense, the *Internet Governance Strategy 2016-2019* is among the first publications on this topic, attempting to guarantee that public policy for the internet is centred on people and tries to promote online democracy and safeguard users and their human rights (Council of Europe, 2016).

The strategy is one of the most avant-gardes in digital rights. It is the result of constant effort, including other instruments that are directly or indirectly relevant to digital rights protection, such as the *Privacy and Electronic Communications Directive 2002*, *Communication 532 on Copyright in the Knowledge Economy* (2009), the *Declaration on Internet governance principles* (2011), among others (see Figure 6).

Figure 6. Chronology of the Evolution of European Union Legislative Instruments



Source: Author's elaboration with data from Karsten (2013) and Parliamentary Assembly (2019)

As seen in the preceding timeline, legislative action has recently increased, particularly in 2014, when committee recommendations prioritise protecting personal data and human rights online (Karsten, 2013).

The establishment in 2008 of the European Dialogue on Internet Governance (EuroDIG) has provided a platform for a lively conversation on governance, also open to citizen participation (European Dialogue on Internet Governance, n.d.). Additionally, in the document *Regional Internet Governance and Policy Europe's Influence on the Future of Internet Governance* (2014), the European Union makes explicit its direction toward a governance model that aims to enhance the multi-stakeholder model, which consists of three crucial parts: 1)

inclusiveness, 2) transparency, and 3) accountability (European Commission, 2014).

To defend human rights, the Parliamentary Assembly has also published some recommendations regarding allocating responsibilities to search engines and social networking services. Meanwhile, for its part, the 2011 *Declaration of Governance Principles* has been one of the most noteworthy mechanisms of digital rights protection (Parliamentary Assembly, 2019).

Concerning the liability limits, It is crucial to mention Articles 12, 13 and 14 of the *e-Commerce Directive*, which outlines the conditions under which Internet Service Providers cannot be held responsible for the actions of third parties (European Parliament of the Council, 2000). These exclusions contain three requirements for ISP involvement: 1) mere conduct, 2) caching and 3) hosting. Table 2. summarises the criteria for receiving "safe harbour" benefits.

Table 2. Exceptions to ISP liability for the activity of third parties under Articles 12, 13 and 14 of the e-Commerce Directive

Exception	Details
Mere conduit	ISPs cannot be held liable if they do not: ➢ Initiate the transmission ➢ Select the receiver of the transmission ➢ Select or modify the information contained in the transmission
Caching	They cannot be held liable for caching if they: ➢ Do not modify the information ➢ Comply with rules regarding the updating of information ➢ Do not interfere with the lawful use of technology ➢ Do not modify the information
Hosting	ISPs are not held liable for performing if: ➢ Do not have knowledge of illegal activity or information and

	are not aware of facts or circumstances ➢ They act expeditiously to remove or disable access to the information

Source: Author's elaboration with information from European Parliament of the Council (2000)

Regarding the removal of material, Article 15 of the directive states:

> *"Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity. "* (European Parliament of the Council, 2000, p. 13)

The assigned duties seek to safeguard copyrights and prevent criminal activity on the internet, such as child pornography, organised crime, radicalisation, and other illegal acts. These instruments establish several "safe harbours" (see table 2) that, when implemented by ISPs, absolve them of liability for activities committed or assisted through their services.

Another rule concerning ISPs' obligations is the *Data Protection Directive,* which applies to active internet intermediaries, who are deemed data controllers within the definitions of the *Data Protection Directive* since they determine the purpose and methods of data processing (Van der Sloot, 2015). Internet Services Providers must also comply with the rules of the *General Data Protection Regulation*, depending on their degree of activity (Van der Sloot, 2015).

Due to the degree of involvement in the distribution and access to information, the *European Convention on Human Rights* also relates to the ISPs' liability, as it comes into play when user information is shared with government agencies. In such cases, ISPs may utilise this legal

instrument to defend themselves against demands for communications monitoring and customer data sharing (Van der Sloot, 2015).

Concerning the bodies and individuals responsible for all these instruments' implementation, the Vice-President for the Digital Single Market plays a crucial role in developing internet policies. The Commissioner for the Digital Economy and Society coordinates the Directorates-General for Connectivity (Communications, Networks, Content, and Technology) and is directly responsible for policymaking in the ICT sector. National Regulatory Authorities (NRAs), BEREC, the European Commission, the Competition Commissioner, Directorate-General Informatics, and Directorate-General Internal Market and Services, among others, are also involved (Savin, 2017).

As they are designed to combat certain online behaviours, these regulations have implications for exercising freedoms. Therefore, for Human Rights protection, the responsible bodies are the Council of the European Union, which oversees these matters but also democracy and the rule of law. The European Court of Human Rights (ECtHR) also plays a critical role (Savin, 2017). As noted, the liability regime offers a variety of protections to prevent ISPs from being overburdened with obligations.

Generally, the regime interacts with other instruments, such as digital markets, personal data management, human rights, privacy, and intellectual property. This complexity is reflected in the limitations and challenges discussed in detail in the following section.

5.3. Scope and Limitations

Despite the EU's significant contributions, there are several weaknesses and limitations relating to the burden of responsibility on Internet Service Providers, notions of transparency and accountability, the

implementation of safeguards and intelligence agencies' activities require attention.

- **ISPs' burden of responsibility**

As stated, the *e-Commerce Directive* outlines ISP obligations and liability exemptions. Nonetheless, some flaws are associated with the directive's coverage of the notice requirement, content blocking mechanism, freedom of speech, and unfair competition (Madiega, 2020).

Concerns also relate to the policing duties that ISPs must undertake to comply with the legislation and get access to the "safe harbour" (Madiega, 2020). The economic and technological consequences of an excessive burden can potentially affect the operability of ISPs and lead to adopting technologies such as pre-posting filters (Madiega, 2020).

On this, Marusic (2016) notes the importance of distinguishing between ISPs' responsibilities in economic and human rights terms since the content of each discussion differs significantly.

- **Transparency and accountability**

The *Internet Governance - Council of Europe Strategy 2016-2019* calls for establishing a dialogue platform that includes diverse actors involved in protecting human rights to discuss accountability and transparency principles concerning collecting, storing, and analysing personal data. The initiative, mentioned earlier, is designed to ensure that incidents of human rights violations get enough attention (Council of Europe, 2016).

In the *Guide to Human Rights for Internet Users*, the private sector is urged to engage in a genuine dialogue with state authorities and with members and representatives of civil society regarding their corporate social responsibility in terms of accountability (Council of Europe, 2014). Also, in 2014, in the *Communication Internet Policy and Governance:*

Europe's Role in Shaping the Future of Internet Governance, the commission announced its COMPACT[5] vision for internet governance (European Commission, 2014).

Specifically, the 2022 *e-Commerce Directive* establishes harmonised standards for openness and disclosure obligations for online service providers, commercial communications, electronic contracts, and restrictions for intermediary service providers (European Commission, 2022b).

Observably, there is a growing interest in principles such as openness and responsibility related to private sector participation in internet governance and data management. However, there is a lack of concrete mechanisms and measures to ensure: 1) regular and effective accountability, such as the publication of annual reports on the number of requests for personal data by government institutions, 2) a greater impetus to a multi-stakeholder dialogue where ISPs can defend their interests and establish limits to their responsibilities, and other sectors such as organised civil society can share their concerns, and 3) the establishment of a body specifically charged with the protection of digital rights.

- **Safeguard implementation**

Currently, no concrete protections are in place to provide the private sector with the means to defend itself against government demands for information. It is known, for instance, that ISPs may use the European Convention on Human Rights (ECHR) if they do not want to disclose

[5] COMPACT is the European Union's proposal for "the Internet as a space of Civic responsibilities, One unfragmented resource governed via a Multistakeholder approach to Promote democracy and Human Rights, based on a sound technological Architecture that engenders Confidence and facilitates a Transparent governance both of the underlying Internet infrastructure and of the services which run on top of it" (European Commission, 2014).

customers' personal information to third parties or refuse to monitor conversations (Van der Sloot, 2015).

However, there is a need for a clearer understanding of the resources and methods by which ISPs may apply safeguards to their digital governance obligations and collaboration with law enforcement authorities when their interests and users' rights are at risk. These measures can also be used in cases where the copyright enforcement responsibilities require too much from ISPs and do not provide concrete steps for removing content or contravening the ISPs' operations (Lesiak, 2009).

- **Intelligence agencies' activities**

As mentioned, the *Human Rights Guide for Internet Users* includes exceptions to the exercise of digital liberties. In particular, it states that although the interception of communications affects the right to privacy, such a power is subject to the restrictions set out in Article 8, paragraph 2 of the *European Convention on Human Rights* (Council of Europe, 2014). The exemption involves the following circumstances:

> *"*[...] *in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."* (European Court of Human Rights, 2021, p. 11)

Although the guide makes it clear that the mere existence of a legal instrument permitting telecommunications surveillance can be considered an infringement of the right to privacy, it also provides a series of measures that governmental authorities must adhere to when acting under the exceptions stated above. These measures include foreseeability, essential safeguards for discretion by public authorities,

and monitoring and review by designated authorities (Council of Europe, 2014). Although the steps are reasonable, they are merely recommendations; thus, each state must determine whether or not to implement them.

Experts, such as Morin-Desailly (2014), have also examined the need to improve the regulation of intelligence agencies. Morin-Desailly (2014) advocates updating legislation to improve legal supervision of intelligence services' activities. The plan proposes the establishment of an independent commission to supervise agencies and review the proportionality of the measures they take (Morin-Desailly, 2014). Within this model, the proposed commission must analyse the legality of intelligence collection activities and approve them (Morin-Desailly, 2014).

The issue discussed above is an ongoing debate involving the quest for a balance between national security and individual liberties, where democracies must balance their responsibilities to safeguard and the rights to privacy and access to information (European Internet Foundation, 2009).

- **Digital Rights**

Concerning the preservation of digital rights, the European Union stipulates in the first section of the *Declaration on Internet Governance Principles* (2011) that: "Internet governance arrangements must ensure the protection of all fundamental rights and freedoms and affirm their universality, indivisibility, interdependence and interrelation in accordance with international human rights law" (Council of Europe, 2011). It also adds: "All public and private actors should recognise and uphold human rights and fundamental freedoms in their operations and

activities, as well as in the design of new technologies, services and applications" (Council of Europe, 2011).

Additionally, the *Guide to Human Rights for Internet Users* outlines the responsibilities of member states to defend the human rights and fundamental freedoms of all individuals subject to their jurisdiction, following the *European Convention on Human Rights* (Council of Europe, 2014). In this sense, the document notes that nobody on the internet should be subjected to unlawful, unwarranted, or excessive interference with their fundamental freedoms (Council of Europe, 2014).

Moreover, it states that users should receive information on the exercise and protection of their online rights, which are also specified in the document (Council of Europe, 2014). Despite the declaration and the guide covering various aspects, it lacks specificities such as dispute management mechanisms and the resources available to citizens when their rights have been violated. In general terms, there is a lack of greater disclosure and clarification of the mechanisms for reporting and/or initiating complaints, as well as the scenarios that may constitute an infringement of digital rights.

- **Net neutrality**

Since 2002, legal instruments on telecommunications have been developed to take basic measures for net neutrality, namely the *Council of 25 November 2009 amending Directives 2002/21/EC on a Common Regulatory Framework for Electronic Communications Networks and Services* and *Directive 2009/140/EC of the European Parliament* (Savin, 2017).

However, formal debates on net neutrality did not begin until 2009, as a consequence of 1) legislative proceedings centred on the Telecoms Package process and 2) public pressure that culminated in a public

seminar on net neutrality and a consultation process (Horten, n.d.). Nevertheless, no tangible result was reached (Horten, n.d.).

In 2014, the European Parliament introduced several rules to include net neutrality into the European Union statutes (Horten, n.d.). In June 2016, BEREC published *Guidelines on the Implementation by National Regulators of European Net Neutrality Rules*. The document stipulates in further detail that non-preferential management of traffic, and no different pricing from the traffic transmission, are necessary elements to ensure users' rights (BEREC, 2016).

In May 2022, updated guidelines on implementing regulations for the open internet were released based on the outcomes of the 2019 public consultation (Defraigne, 2022a). The most significant conclusion about pricing differential when traffic is handled equally is that: "the CJEU [Court of Justice of the European Union] interpretation on zero-rating leaves room for differentiated billing practices under the scope of application of Article 3(2) of the Regulation" (The European Consumer Organisation, 2022, p. 1).

According to the above, since zero-rated offers lead to price differentiation, regardless of limitations, they are incompatible with the equal traffic obligation in Article 3.3 of the regulation (The European Consumer Organisation, 2022).

Lastly, the *Telecommunications Single Market (TSM)* allows for banning apps, applications, content, and terminal equipment, charging a premium tariff for specific applications, and the payment of various bandwidths or data restrictions(Defraigne, 2022b). However, there are a few exceptions, such as 1) when national and/or EU rules must be followed, 2) network security must be maintained, and 3) network congestion must be avoided (Defraigne, 2022b).

In conclusion, the European debate on net neutrality continues to evolve. It is undergoing a period of particular significance, where both the CJEU and the National Regulatory Authorities (NRAs) will have to delve deeper into various questions such as end-user filtering services and the transparency mechanisms to be adopted for internet traffic management, among other issues, which will undoubtedly appear in the expected final updated BEREC Guidelines (Defraigne, 2022b).

Consensus building and balanced actions on net neutrality are of utmost importance since, as stated before, it is essential to enjoy other digital rights.

5.4. Digital rights challenges

The adoption, updating, and transformation of European legislative tools are positive steps towards the protection of digital rights, as the *Internet Governance Strategy* correctly states: "Everyone should be able to exercise their human rights and fundamental freedoms, including the right to privacy and the protection of personal data, both online and offline" (Council of Europe, 2016, p. 7).

The guide specifically addresses the protection of the right to freedom of expression, access to information, right to freedom of assembly, protection from cybercrime, right to private life, and the protection of personal data, which are also mentioned in other instruments such as the *General Data Protection Regulation* (GDPR), the *ePrivacy Regulation* (ePR), and the *Council of Europe Convention on Cybercrime* that embodies the universality, indivisibility, and interdependence of human rights.

National security efforts in the European Union require checks and balances to ensure equilibrium between the protection of national interests and individual liberties, entailing the dissemination of available

frameworks and accountability and transparency tools. This must be done while keeping in mind the position of ISPs as partners with government entities, which are also required to follow human rights laws.

Scarlet Extended v. SABAM and SABAM v. Netlog are two cases involving ISPs' duties over copyright and private sector interests. In those cases, the Court of Justice of the European Union (ECJ) determined that requiring ISPs to filter would not be a fair balance between copyright protection and ISPs' interests because it would demand the installation of a highly costly and complex IT system, which is contrary to Article 3(1) of the Directive. The court also acknowledged those measures would affect fundamental rights (Vranckaert, 2020).

The cases underline the importance of constant reflection on the balance between the commercial, law enforcement, and human rights duties of ISPs and the steps necessary to safeguard digital rights.

Chapter 6. The Organisation of American States' case

6.1. Background

In the Americas, the ecology and frameworks on e-governance remain in their infancy. At the regional level, there is significant interest in harnessing and expanding the benefits of the digital economy and integrating technical breakthroughs, but legislative progress is modest (CEPAL, 2020). Most existing internet governance legislation is based on the United States or European Union instruments, which —while a good starting point— respond to different contexts and capacities than those found in the Americas.

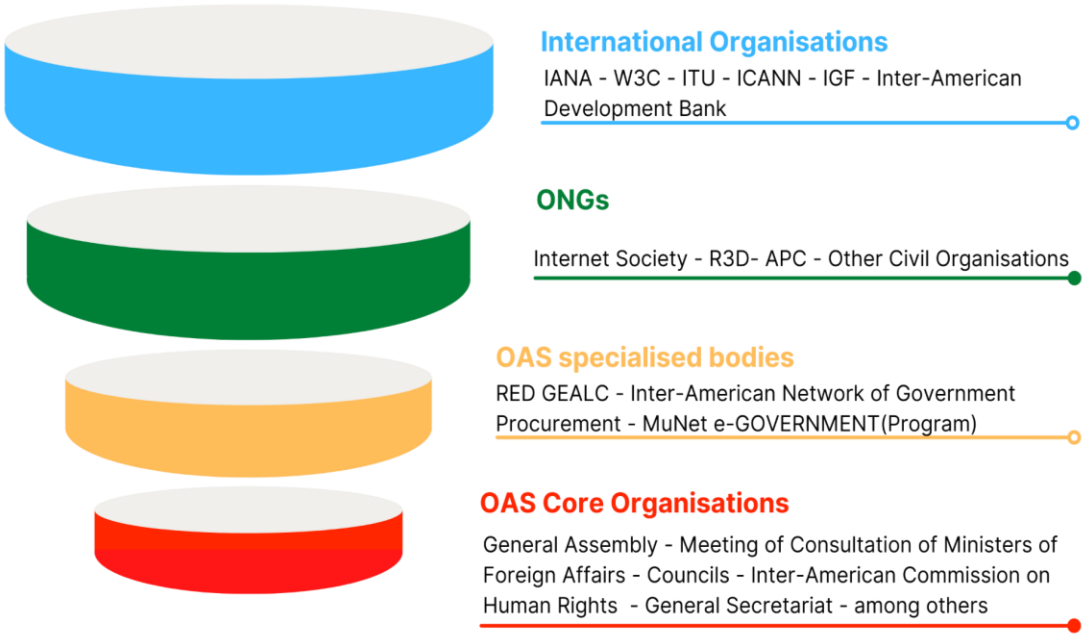
The American continent is characterised by a multitude of organisations that seek to promote the region economically, politically, and socially, including the Association of Caribbean States (ACS), the Latin American Integration Association (ALADI), the Bolivarian Alliance for the Peoples of Our America (ALBA), the Andean Group or Andean Community (CAN), the Caribbean Community and Common Market (CARICOM), and the Community of Latin American and Caribbean States (CELAC). The multitude of collaborations entails a range of agendas, interaction norms, and obligations, thereby rendering a regional and uniform digital governance an arduous objective.

Founded in 1948, the Organisation of American States is the oldest association of nations in the world (OEA, 2009). Its mechanisms and competencies have been transformed over time to achieve leadership status. The OAS is composed of a General Assembly, the Meeting of Consultation of Ministers of Foreign Affairs, the Councils (which includes the Permanent Council, the Inter-American Council for Integral Development), the Inter-American Juridical Committee, the Inter-American Commission on Human Rights, the General Secretariat, the

Specialised Conferences, the Specialised Organisations, among other entities (OEA, 2009).

Regarding internet governance and digital rights, the involved organisations include RED GEALC (Network of e-Government of Latin America and the Caribbean), and the Inter-American Network of Government Procurement, in addition to those already listed. The OAS, with the assistance of the International Development Research Centre (IDRC), the Inter-American Development Bank (IDB), and the Canadian International Development Agency (CIDA-ACDI), as well as programmes such as MuNet e-GOVERNMENT, are working to improve internet governance in the American continent (see Figure 7).

Figure 7. Institutional Ecology (OAS)- Organisations active in internet governance and digital rights protection



Source: Author's elaboration with data from OEA (2009)

Recently, various initiatives and programmes have been launched to enhance internet governance and assist nations in their transition to e-government. However, as mentioned before, most instruments are

based on U.S. or European Union legislation. Therefore, concerns exist over this influence's incapability to address regional challenges. In addition, there are a variety of projects that may conflict with one another (CEPAL, 2020).

Particular note should be made to the OAS incentives for developing and adapting effective legislative frameworks on digital governance, data protection, accountability regimes, human rights, and government capacity building. Currently, the OAS is founded on a paradigm of horizontal cooperation, strategic partnerships, and several regional development initiatives (OEA, 2010).

6.2. Type of liability regime

The Americas remains a relatively unexplored region compared to the academic attention given to liability regimes and e-governance legislation in Europe and the United States. Few nations have a defined regulation for intermediaries (Wegbrait, 2014).

Recognising that internet intermediaries deserve special legal protection due to their crucial role in the internet's operation has been the regional approach over time (CEPAL, 2020). However, challenges in the region, such as explicit violence on the internet, the disclosure of intimate images, disinformation, copyright infringement, terrorism, and organised crime on the internet, have led to rigid legal frameworks. The above has eventually led to assigning greater responsibilities to ISPs (CEPAL, 2020).

A fragmented approach characterises the American continent. All OAS members have different tools established at different times, with Canada and the United States as the leaders in legislative preparedness. Elsewhere on the continent, intermediaries are often governed by laws based on general administrative, civil, or criminal legislation (Froncek et

al., 2020). For instance, some current copyright laws predate the rise of internet use and, as a result, are insufficient and lack appropriate measures to reinforce them (Froncek et al., 2020).

Liability regimes have developed mainly in response to economic interests and the protection of copyrights (BID, 2020). As a result, safeguards for rights such as freedom of communication and information and net neutrality are in their early stages.

Until 2020, for instance, Argentina, Uruguay, and Mexico lacked a complete and enforceable legislative framework for ISP responsibility, relying instead on alternative legal tools for third-party damages (BID, 2020).

Since the OAS recommendations are not binding, ISPs perform state functions in many countries, such as classifying content as legal and illegal and removing the latter (CEPAL, 2020).

Consequently, the regional landscape ranges from liability regimes that provide "safe harbours" for ISPs to more stringent frameworks. Such is the case of the Bolivarian Republic of Venezuela and the Republic of Cuba, where ISPs are required to monitor and regulate content, and states exert substantial control over communications (CEPAL, 2020). While in other countries, ISPs are responsible for combating crimes such as hate speech or adopting strict measures to comply with their legal obligations (CEPAL, 2020).

There is broad concern about the potential consequences of this disproportionate burden on democratic nations. Nevertheless, problems such as misinformation in electoral contexts emerge as pressing issues that lead to the provision of policing functions to intermediaries (CEPAL, 2020). Table 3 shows some OAS members with liability regimes or related.

Table 3. Some liability regimes for Internet Service Providers in some OAS countries

Country	Year	Legal instrument
Argentina	2015 / 1968/ 1933	Civil and Commercial Code/ Civil Code / Intellectual Property Law
Bolivia	2011	Law No. 164, on Telecommunications, Information and Communication Technologies
Brazil	2018 / 2014	Law n. º 13.709, General Data Protection Law / Marco Civil da Internet - "Brazilian Civil Rights Framework for the Internet"
Canada	2018 / 2017/ 2012	Elections modernization Act/ Copyright Act/ Copyright Modernization Act /
Chile	2010	Law No. 20.453 establishing the principle of Net Neutrality for consumers and Internet users and Law No. 20.435 on Copyright
Colombia	2006	Law No. 679 by which a statute is issued to prevent and counteract exploitation, pornography, and child sex tourism, implementing Article 44 of the Constitution
USA	2018 / 2012/ 2010 / 1998	Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA) / Trade Acrt / Speech Act / Digital Millennium Copyright Act
Guatemala	2013	Copyright Law, Decree No. 33-89
Mexico	2020 / 2014 / 2013 / 2010	Mexican Federal Copyright Act / Broadcasting and Telecommunications Act / Civil Code /Federal Law of Personal Data Held by Private Parties
Peru	1996 / 1984	Decree 822 Copyright Law and Decree 295 Peruvian Civil Code
Trinidad & Tobago	2011	Electronic Transactions Act, No. 6

Source: Author's elaboration with data from The Centre for Internet and Society (2018).

As shown in Table 3, a significant share of the legal instruments used for ISP liability is almost eighty-year-old copyright and telecommunications legislation. Although some of these legal instruments are regularly updated, they leave a gap in their coverage of the digital dimension of these activities and the regulatory mechanisms required to govern them.

The conclusion of free trade agreements with other nations has boosted liability regimes in some countries, such as Colombia (The Centre for Internet and Society, 2018).

Another factor that has influenced the development of instruments is the European Union's General Data Protection Regulation (GDPR). Since its entry into force in 2016, laws related to data protection have been passed in Argentina, Chile, Colombia, and Uruguay, and others have initiated law reform in this area (CEPAL, 2020).

Concerning protecting personal data, it is essential to mention the *Habeas Data* principle. *Habeas data* consists of the right to access personal data, a common inheritance of Inter-American constitutional law, therefore most states' constitutions recognise it substantively or procedurally (Botero Marino, 2013). This right is also articulated in section 3 of the Organisation of American States' *Declaration of Principles on Freedom of Expression*, which states:

> *"Every person has the right to access to information about himself or herself or his/her assets expeditiously and not onerously, whether it be contained in databases or public or private registries, and if necessary to update it, correct it and/or amend it"* (OAS, 2017).

The OAS further adds that obtaining data should be straightforward, not require justification by the claimant, and be free of charge (OAS, 2017).

If there is a barrier to this right, it must fulfil norms of necessity and proportionality (OAS, 2017).

With the proliferation of organisations capable of collecting, storing, and analysing data, the *Habeas data* assumes a new dimension. Nevertheless, in the Americas, the obligation of intermediaries varies from nation to nation.

At the regional level, the OAS influences national legislation via initiatives, recommendations, and reports on various issues, including freedom of speech, privacy, and personal data protection, which are discussed in detail in the following section.

6.3. Scope and Limitations

The greatest challenge at the regional level is the homogenization of legislative norms. The political, cultural, economic, and social variety of the 35 member states creates a complex environment. Moreover, the different pace of adoption of standards directly impacts the feasibility of establishing uniform liability regimes.

Generally, there is an imbalance between legal regulation of online activity and everyday reality. This circumstance is exploited by players such as organised crime and totalitarian governments, who have transformed the web into another venue for exercising power and dominance.

The context in which these harmful behaviours have flourished is characterised by a lack of coordinated regional action, limited public knowledge of digital rights, and ineffective coordination between the public and commercial sectors (IEEE, 2017). Despite the above, the Organisation of American States holds a unique position in terms of guidance for its members. Documents concerning freedom of

expression, fake news, and misinformation, among others, are among the most relevant in this respect (see Table 4).

Table 4. OAS tools on digital rights and intermediaries' liability

Year	Name
1969	American Convention on Human Rights "Pact of San José, Costa Rica"
2009	Press Release R50/11 - Freedom of Expression Rapporteurs Issue Joint Declaration Concerning the Internet
2011	Joint Declaration on Freedom of Expression and the Internet
2012	UN and IACHR Special Rapporteurs for Freedom of Expression Joint Declaration about Free Speech on the Internet
2013	Joint Declaration on Surveillance Programs and their Impact on Freedom of Expression
2013	Freedom of Expression and the Internet (OAS Report)
2017	Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda
2017	Standards for a Free, Open and Inclusive Internet
2019	Guide regarding Deliberate Disinformation in Electoral Contexts
2019	Joint Declaration on Challenges to Freedom of Expression in the Next Decade
2020	Joint declaration on freedom of expression and elections in the digital age
2022	Updated Principles on Privacy and Personal Data Protection. AG/RES. 2974 (LI-O/21)

Source: Author's elaboration with data OAS (n.d., 2009a, & 2022) and OEA (2019).

In addition to the documents listed in Table 4, others, such as those produced by the Inter-American Development Bank, the Economic Commission for Latin America and the Caribbean, and the Latin American Internet Association, focus on ISP accountability and the implications of adopting strict regulations for human rights (Bustos Frati et al., 2021; CEPAL, 2020, and BID, 2020).

However, the OAS documents are merely guidelines and recommended standards. In the case of the Inter-American Court of Human Rights, there is a capacity to follow up on its recommendations. However, the court acknowledges it requires further capacity building to ensure effective compliance with its decisions and recommendations concerning the observance of human rights in its member states (OEA, n.d.).

In internet governance, the OAS publications mentioned above assess the most pressing difficulties in the region, including those on ISPs' liability load, transparency and accountability, implementation of safeguards, intelligence agency operations, and digital rights (OEA, 2013b).

- **ISPs' burden of responsibility**

For the Organisation of American States, internet intermediaries are vital for the transmission of ideas, access to information, culture, and education, as well as for regional prosperity (Botero Marino, 2013).

The OAS also acknowledges that both states and private actors have sought to exploit the position of ISPs, using them as control points, and refers: "[it is because] it is easier for States and private actors to identify and coerce intermediaries than those directly responsible for the expression they seek to inhibit or control" (Botero Marino, 2013, p. 40). The OAS also notes: "There is also greater financial incentive in seeking to impose liability on an intermediary rather than on an individual user" (Botero Marino, 2013, p. 40). This circumstance has prompted several nations to set tight liability regimes on ISPs, making them liable for the actions of third parties (Botero Marino, 2013).

In particular, the *Joint Declaration on Freedom of Expression and the Internet* states that:

> *"*[n]*o one who simply provides technical Internet services such as providing access, or searching for, or transmission or caching of information, should be liable for content generated by others, which is disseminated using those services, as long as they do not specifically intervene in that content or refuse to obey a court order to remove that content, where they have the capacity to do so (‘mere conduit principle’)"* (OSCE, 2011, p. 2).

The OAS is aware that the obligations of ISPs may exceed their capacities and that this opens the door for governments and the private sector to increase their demands on intermediaries because exerting control over a large number of users is less feasible. Although the organisation explicitly recognises these facts, its recommendations are not binding on states. However, they serve as a benchmark for what should prevail in the digital world.

In general, it is necessary to extend the evaluation of ISP issues and to organise forums where they may also voice their concerns to develop a multi-stakeholder discussion to improve procedures and counteract abuses.

- **Transparency and accountability**

In terms of transparency and accountability, the *Standards for a free, open, and inclusive internet* mandates that ISPs: "should put in place effective systems of monitoring, impact assessments, and accessible, effective complaints systems to identify actual or potential human rights harms caused by their services or activities" (OAS, 2017, p. 43). Furthermore, the document adds:

> *"Where negative human rights impacts or potential impacts are identified, private actors should have in place effective systems for providing appropriate remedies for those affected; and adjust their activities and systems*

> *as necessary to prevent future abuse.* [...] *private actors should adopt robust approaches towards transparency in relation to their terms of service, policies and any operating procedures or practices which directly affect the public"* (OAS, 2017, p. 43).

The document also urges ISPs to clarify their content removal procedures. It also highlights the efforts of the UN Special Rapporteur to advocate for transparency in decision-making to avoid discriminatory practices and political pressure that might influence business choices (OAS, 2017).

The OAS' openness and accountability measures prioritise the preservation of free speech, personal data, and privacy. The agreements include advice on what ISPs should prevent and governments' responsibilities for human rights protection.

Despite substantial research on the topic, there is no best practice guide to inform regional ISPs of their duties and the extent to which states can hold them accountable for compliance with various standards.

A positive step toward transparency would be ISPs and states collaboration to make public the decision-making process for blocking and removing online content and how individuals can appeal these decisions.

- **Safeguard implementation**

The Inter-American Commission on Human Rights emphasises the importance of safeguards in preventing abuses. (OAS, 2009b). The document *Freedom of expression and the Internet* stipulates that authorities must establish safeguards for ISPs to operate transparently and that governments must also provide conditions for them to serve as

conduits for the enjoyment of the universal right to freedom of expression (Botero Marino, 2013).

In 2013, Edward Snowden's revelations led to the *Joint Declaration on surveillance programmes and their impact on freedom of expression*, in which the Organisation of American States (OAS) asserts that intermediaries must endeavour to ensure that users' rights and data are protected and that everyone has unrestricted access to the internet. In addition, the declaration urges businesses not to deploy surveillance technologies that violate users' rights (OEA, 2013a).

As noted, the region has a clear political will to provide ISPs with safeguards. However, as mentioned above, there is no protocol or action guide to which ISPs can turn when states entrust them with tasks that are beyond their capabilities or may violate human rights. It is vital to provide procedures for the parties concerned to equalise rights and duties.

- **Intelligence agencies' activities**

Limitations on intelligence agencies' activities in the Americas are solely the responsibility of national governments. However, the OAS mandates in the *Joint Declaration on Freedom of Expression and the Internet* that legislation providing for state monitoring of communications must clearly and succinctly express its grounds, and a court must authorise these actions (Botero Marino, 2013). Furthermore, these measures should specify the kind, extent, and duration of surveillance, the conditions under which it is authorised, the authorities accountable for it, and the means available to combat abuses (Botero Marino, 2013).

The OAS' stance on the proper exercise of monitoring obligations also includes compliance with regional instruments that obligate OAS members to observe human rights, such as the American Convention on

Human Rights, which stipulates in article 11: "[n]o one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honour or reputation" (IACHR, 2009). States are, therefore, bound to respect citizens' privacy and protect them from the activities of third parties (Botero Marino, 2013).

Likewise, the regional organisation emphasises the concept of national security must be consistent with a democratic society. The OAS deems it illegitimate to intercept, seize, or exploit private information of dissidents, journalists, and human rights activists for political objectives or to obstruct or undermine their investigations or denunciations while citing the defence of national security (Botero Marino, 2013).

The OAS recognises that governments and agencies can negatively exploit the concept of national security in various contexts and, consequently, imposes necessary safeguards when claiming national security defence. The organisation is well aware of the new dimensions that surveillance tasks take on in the digital age and stipulates that illegal surveillance, interception, and acquisition of personal data threaten both the right to privacy and the freedom of speech and the fundamental principles of democratic societies (OAS, 2017).

While the Snowden revelations resulted in the mentioned earlier joint declaration, more dialogue is needed between governments to extend commitments and adopt transparency and accountability mechanisms. Likewise, individuals need a greater understanding of the legal tools for taking allegations of abuse to court.

The Inter-American Court of Human Rights is authorised to render judgments against the parties concerned, including states. Still, the difficulty of implementing its recommendations persists due to the

organisation's nature and the lack of mechanisms to monitor its progress.

- **Digital Rights**

The legacy of power abuses, military and authoritarian regimes, and human rights violations throughout the region —notably during the 1960s and 1970s— has made safeguarding human rights a constant concern in all OAS statements and recommendations. Apart from recent incidents of corruption,[6] political espionage, and the existence of authoritarian governments, abuse precedents have given birth to an active and organised civil society, as well as a wave of human rights activism in the digital sphere.

Despite the constant regional dialogue on the matter, the Inter-American Commission on Human Rights notes that several states have acquired or are acquiring surveillance technology (OAS, 2017). The above is a worrying trend due to the absence of legal frameworks for its regulation. The Inter-American Commission on Human Rights also notes: "States must demonstrate need for any measure that keeps certain information secret to protect national security and public order" (OAS, 2017, p. 84).

Regarding the data collection for national security purposes, the IACHR cites the *Johannesburg Principles on National Security, Freedom of Expression, and Access to Information*[7] and notes that confidentiality must hold a justified and legitimate purpose (OAS, 2017).

An essential aspect of the OAS' efforts is that it envisions the involvement of an independent and specialised agency in situations of

[6] For example, the Odebrecht case, which involves a Brazilian construction company that paid bribes to officials in at least 12 countries, including Brazil and Peru, Ecuador, Argentina, Colombia, Guatemala, Panama, the Dominican Republic and Venezuela, but which also has ramifications in Angola and Mozambique in Africa, and in the United States. Source: El Universal (2019).

[7] Their goal was to set authoritative standards clarifying the legitimate scope of restrictions on freedom of expression on grounds of protecting national security. The principles were adopted by a group of experts in October 1995. Source: Article 19 (2003)

rights limitation. The OAS proposes an agency with technological competence and safeguards to maintain the internet's and communications' integrity (Botero Marino, 2013).

In addition to *Habeas data,* diverse nations have enacted special legislation to safeguard personal data (Botero Marino, 2013). In contrast, others do so indirectly through regulations controlling traditional forms of communication, as illustrated in Table 3.

- **Net neutrality**

At the regional level, the *Joint Declaration on Freedom of Expression and the Internet* refers that: "[s]hould be no discrimination in the treatment of Internet data and traffic, based on the device, content, author, origin and/or destination of the content, service or application" (Botero Marino, 2013, p. 11). The above is intended to guarantee that users have unfettered access to lawful material, free from any blocking, filtering, or intervention (Botero Marino, 2013).

Net neutrality is deemed vital for the practice of free speech, following Article 13 of the Inter-American Convention (on the right to freedom of expression) (Botero Marino, 2013). The OAS also points out in *Freedom of Expression and the Internet* that states must adopt laws and establish bodies to enforce the principle of internet neutrality (Botero Marino, 2013).

The organisation has produced documents and suggestions regarding net neutrality and its significance in exercising digital rights. Internationally, Chile stands out as a pioneer in net neutrality legislation. At the same time, the rest of the OAS members have approved legislation on net neutrality, including in some cases such as Ecuador, whose law clearly permits zero-rating (Garrett et al., 2022).

6.4. Digital rights challenges

Multiple aspects, such as the implementation of OAS recommendations and adherence to IACHR orders, comprise the regional difficulties regarding digital rights. The diversity of legal frameworks and methods controlling the internet across the region and the different liability regimes makes collaboration a significant challenge.

In the case of personal data protection, for instance, even though there are regulations in most countries, cooperation is necessary to develop an adequate framework at the regional level (CEPAL, 2020).

It is indeed possible to observe a rise in the number of requests for content blocking in the region, as well as an increase in the adoption of administrative sanctions against ISPs, which may lead to the establishment of rigid regimes (CEPAL, 2020). This trend coincides with several efforts to counteract misinformation and hate speech through content filtering (ECLAC, et al., 2020).

It is important to note how economic treaties have determined the adoption of liability regimes, making it a requirement to conclude agreements (CEPAL, 2020). This tendency, on the one hand, leads to establishing necessary frameworks but, on the other hand, creates a situation in which those laws respond to immediate needs. Consequently, some laws were not drafted with regional context and the level of technological innovation in mind (CEPAL, 2020).

Similarly to Europe, there is an urgent need in the Americas to bring ISPs to the discussion table to address the issues of understanding legal frameworks, developing safeguards and establishing transparency and accountability procedures (CEPAL, 2020).

States and the private sector need to achieve a balance of requirements to avoid imposing on ISPs the need to monitor, censor or remove certain types of information, which is becoming a potential threat to freedoms in the region, as is the situation in Venezuela and Cuba (CEPAL, 2020).

Chapter 7. Comparative Analysis

Comparing the digital ecosystems of different players provides a basis for understanding the condition of internet governance in diverse contexts, the most challenging issues, and a viewpoint on the future.

In both regional debates, the relevance of ISPs is undeniable due to their role in 1) managing the vast amount of data that circulates on the network and 2) strengthening the state in the face of the internet's features.[8]

As has been observed throughout this document, the evolution of tools and technical capacities to regulate online activities and protect rights is occurring at a variable rate, which poses a significant challenge due to the internet's interconnectivity and the proliferation of e-commerce between diverse regions.

Against this background, this section focuses on the comparative analysis between the Organisation of American States and the European Union, identifying strengths, weaknesses, areas of opportunity and future challenges regarding ISP involvement in digital rights protection.

7.1. Organisational nature

When discussing two players such as the European Union and the Organisation of American States, the first aspect to consider is their nature, making it difficult to compare the performance of two elements without similar characteristics.

The first emerged from post-World War II cooperation, which, beginning in 1951 with an alliance for the facilitation of commerce in coal and steel, led to the world's most sophisticated integration process, in which

[8] Which are deterritorialisation, anonymity, and worldwide reach. For more info see Chapter 1.

sovereign governments share a part of their sovereignty (Unión Europea, n.d.) (Comisión Europea, 2013).

The EU has positioned itself as an influential actor on various international issues as a result of treaty-making, membership growth, and the adoption and modification of legal and economic powers. Currently, the legislative process begins with the parliamentary committee and continues until an agreement with the Council is obtained (Parlamento Europeo, n.d.). The European Parliament and the Council are responsible for passing legislation and directives through the ordinary legislative process (Furtak, 2015).

For its part, the Organisation of American States was founded in 1948 in the backdrop of the American continent's Cold War to safeguard the sovereignty and promote democracy among its member states (Municipalidad de Coronado, 2021). Over time, complementing entities devoted to human rights, economic growth, trade, and security has been created, and its legislative, economic, and political powers have been improved (Municipalidad de Coronado, 2021).

Currently, the OAS and its organisations are founded on the collaboration of its members. In contrast to the EU, the level of integration has not yet attained monetary and legislative union, and there is no free trade zone (Furtak, 2015). The above suggests the OAS is not authorised to intervene in matters within the domestic jurisdiction since it possesses no competencies beyond those specified in the *Charter of the Organisation of American States* (OAS & OEA, 2009).

The legislative process begins with the approval of resolutions by the OAS General Assembly and the legislative activities of various bodies, including the Inter-American Juridical Committee (DDI & OEA, 2022).

Although differences in capacities and structures, the OAS and the EU provide a valuable overview of the state of digital rights protection and the situation of ISPs vis-à-vis economic and security demands in the American and European continents. Therefore, the following sections compare the present liability regimes of both organisations.

7.2. Legal framework overview

Although both actors have legislation to guarantee freedom of expression and other human rights, the need to protect personal data became a priority after the Edward Snowden revelations and cases such as Cambridge Analytica.

Although there were already some provisions for data transfer and protection for commercial and security purposes, the processing by intermediaries was a pending dialogue.

Individually, the EU and the OAS have worked diligently to build legislative tools for user protection and liability regimes. Table 5 shows the legal instruments for digital rights protection developed by both actors.

Table 5. EU and OAS Legal Instruments for the Protection of Digital Rights

European Union		Organisation of American States	
Year	Tool	Year	Tool
1948	The Universal Declaration of Human Rights	1948	The Universal Declaration of Human Rights
1950	Convention for the Protection of Human Rights and Fundamental Freedoms	1969	American Convention on Human Rights
1967	The Freedom of Information Act (FOIA)	2010	Model Inter-American Law on Access to Public Information
		2000	Declaration of Principles on Freedom of Expression.
2002	Directive on Privacy and Electronic	2000	Right to information: access to and protection

	Communication		of information and personal data in electronic form
2016	The General Data Protection Regulation (GDPR)	2015	A Legislative Guide on Privacy and Personal Data Protection in the Americas
2014	Guide for Human Rights for Internet Users	2016	Standards for a Free, Open and Inclusive Internet
2016	Digital Single Market Strategy for Europe	-	-
2022	Data Governance Act (DGA)	-	-
2023	The Digital Services Act	-	-

Source: Author's elaboration with data from Furtak (2015), DDI & OEA (2022), Comisión Europea (2013), and International Network of Privacy and Law Professionals, INPLP, (2018).

The legal instruments governing digital rights and liability regimes vary significantly between the EU and the OAS, as seen in Table 5. In contrast to the former, which consists of legally enforceable regulations, strategies, and directives, the latter comprises declarations, recommendations, and guiding principles.

The above enables the EU, for example, to create particular laws on liability and requirements for enjoying "safe harbour" advantages. On the other hand, the OAS has a fragmented strategy that depends on each state's decisions.

In both regions, the *Joint Declaration on Freedom of Expression and the Internet* establishes that providers who solely offer access, search, transmission, and caching services cannot be held liable for third-party material under the mere conduit principle (OSCE, 2011).

7.3. Organic operation

Regarding the bodies devoted to internet governance and responsibilities allocation, regional players draw on agencies and institutions dedicated to protecting human rights, trade, and intellectual property.

In the case of the OAS, the General Assembly, Permanent Council, and Inter-American Commission, among others, collaborate to issue recommendations for preserving free speech, the right to information, and the defence of intellectual property. In contrast, the EU has designated specific organisations for data protection and administrative assistance for diverse regulatory obligations (BEREC, 2015) (Comisión Europea, 2022).

Furthermore, both actors participate in international organisations and forums such as the Internet Governance Forum, ITU, and ICANN as a group of nations or at the individual level.

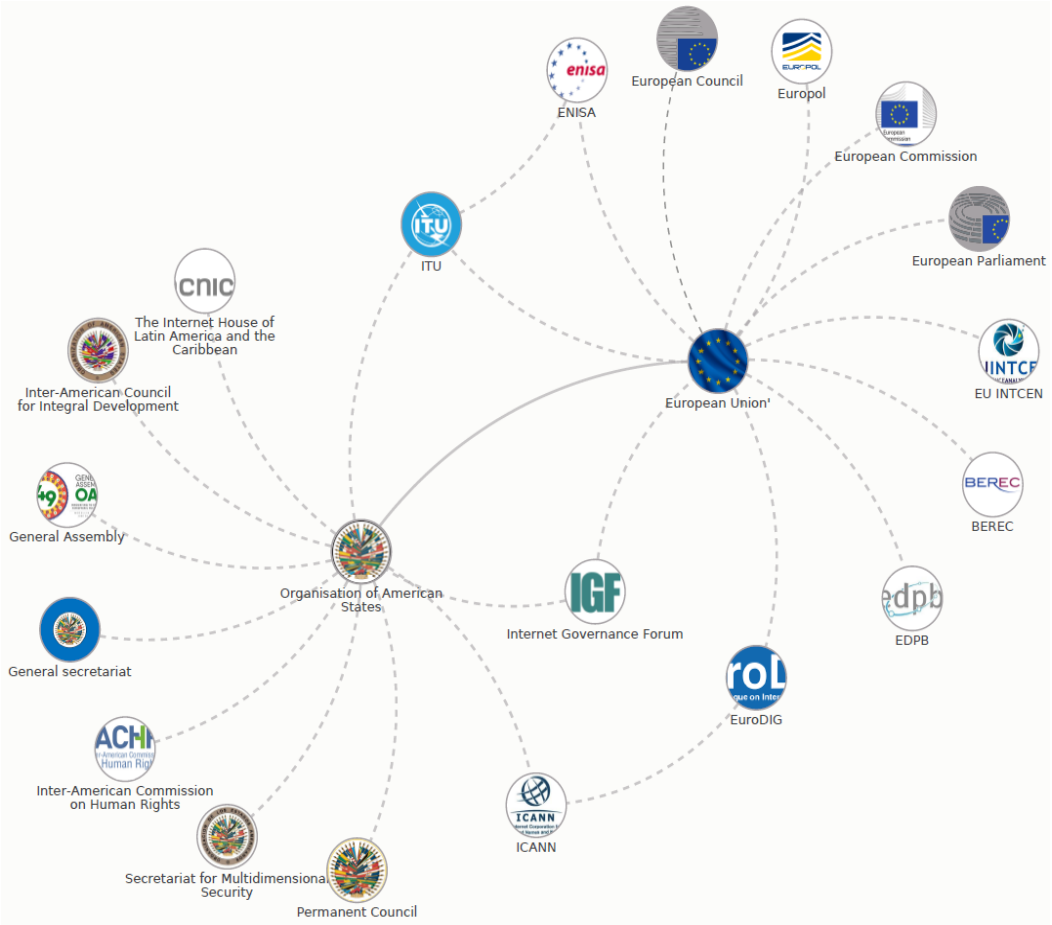
Due to the level of integration within the OAS, security and intelligence operations are conducted solely by national agencies. Although, in the past, the OAS' Secretary for Multidimensional Security made efforts to propose a cybersecurity policy (OEA, 2015).

In terms of actual capacities, the OAS is merely a forum for political, legal, and economic dialogue. Hence it does not have intelligence or security services like the EU. Nor does it have bodies such as the Coordinated Supervision Committee, which among other things, is in charge of supervising personal data transmission between the national Data Protection Authorities (DPA's) and Europol in accordance with *Regulation (EU) 2022/991* (EDPB, n.d.) (Official Journal of the European Union, 2018).

Nonetheless, the OAS has taken significant steps toward greater collaboration, including an agreement with the Latin American and Caribbean Internet Address Registry (LACNIC) to strengthen cybersecurity. This agreement aims to enhance cooperation between governments, the private sector, and civil society to develop a multidimensional approach to cybersecurity (CN-CERT, 2022).

Figure 8 depicts both organisations' architecture and networks. The image shows that the OAS and the EU are intertwined, as the OAS granted observer status to the EU (EU-LAC, 2019). Furthermore, the Organisation of American States and the European Union collaborate closely to strengthen the international human rights framework (Fundación Carolina, 2018).

Figure 8. Organic Dynamics in the European Union and the Organisation of American States



Source: Author's elaboration with data from (Portal de Administración Electrónica, 2022)

It can be observed in Figure 8 that ENISA interacts with ITU since they work on best practices in legislation, organisation, capacity building and collaboration for cybersecurity with the member states (ITU, 2022).

ENISA also adheres to the *General Data Protection Regulation* (GDPR) and the *Digital Single Market* (DSM) strategy and promotes data protection measures through the Privacy by Design concept[9] applied to new electronic products and services (ENISA, 2022).

For its part, the European Data Protection Board is responsible for ensuring the protection of personal data when cooperating with other countries, such as the security cooperation agreements with the United States (Meltzer, 2020).

Cases such as Schrems II illustrate the need for supervision in this field. The case was brought before the European Union's Court of Justice by Maximilian Schrems due to Facebook's failure to protect data transferred from Ireland to the United States. On this occasion, the data was susceptible to the activities of US intelligence services, and the "Privacy Shield"[10] proved to be insufficient (Statewatch, 2022) (Peruzzotti, 2020).

7.4. Regimes Comparison

As discussed in the preceding chapters, the European Union establishes in the *e-Commerce Directive* several conditions for ISPs to access "safe harbour". In addition, at the regional level, the GDPR represents the 27 members with a set of principles, which are supported by the member states at the national level (Daigle, 2021).

In contrast, the situation in the American continent is complicated, with various policies that occasionally accept the "safe harbour" or are based on traditional laws regarding third-party damages or copyright protection. In the case of the United States, Mexico, and Canada, the T-MEC trade

[9] Within the framework of the GDPR, it refers to data protection through technology design. Source: Intersoft Consulting (n.d.)

[10] A framework constructed by the US Department of Commerce and the European Commission to enable transatlantic data protection exchanges for commercial purposes. Source: (Thomson Reuters., 2022)

agreement set rules for protecting online platforms from third-party content (Whitmore et al., 2021).

The legislative variety is not unique to the American continent; other regions, including Africa and Asia, face the same difficulties. In the case of Africa, it has been recommended to establish pan-African data protection and privacy policy. These policy measures might also be replicated in the Americas (Daigle, 2021).

7.5. Status of digital rights

Digital rights are protected in the EU by various laws. Nevertheless, capacity-building efforts are essential to assist ISPs in understanding their current legal obligations. This measure can be beneficial since the European Union does not have a specific framework for taking down content. It delegates to the courts of each state the adoption of preventive measures (OPBP, 2021). A noteworthy exception is the *Directive on Combating Terrorism*, which requires intermediaries in all member states to remove terrorist-labelled content within an hour of receiving the order from the competent authority (OPBP, 2021).

On the other hand, digital rights raise significant challenges for the OAS, ranging from the co-optation of media and infrastructure by non-democratic regimes to a lack of trust in building national security data-sharing channels.

While the *Habeas data* doctrine is predominant in the Americas and provides the highest constitutional protection to citizens, it may be insufficient in some cases because it does not provide an adequate level of security compared to, — for example, the GDPR (Guadamuz, 2001). Nonetheless, in a varied region with a lack of legal uniformity, *Habeas data* is the most potent recourse (Guadamuz, 2001).

Over the past decade, there has been a transition from *Habeas Data*-inspired models to EU-inspired regulations (Villegas Carrasquilla, 2012). This influence makes the new instruments incapable of providing adequate protection (Villegas Carrasquilla, 2012).

In general terms, the absence of homogeneity and a shared vision persists as a problem in the American landscape. Furthermore, Latin America's history of human rights violations makes preserving free expression and personal privacy a regional priority. Achieving these goals requires progress in internet governance, clarifying intermediary duties, and increasing public awareness of how digital rights can be protected.

Whether in the OAS or the EU, the lack of inclusion of ISP concerns regarding accountability regimes stands out. It is, therefore, necessary to open spaces for dialogue between the private sector, state representatives, organised civil society, and citizens to address each region's particular demands.

Likewise, it is strongly recommended that ISPs report on government information requests made under the guise of national security. Citizens need to be informed of the conditions under which personal data may be shared and processed in the interests of national security and the scope and limits of intelligence agencies' operations.

7.6. ISP vs national' security demands

One of the most vexing issues in both regions is the role of ISPs in national security: both the Americas and Europe broadly recognise the protection of digital rights, but they also recognise their restriction when national security is at stake.

Little is known regarding the quantity of data agencies may be accessed, whether a judge's consent is required —in certain American nations—, how long they can retain data, and the extent to which ISPs must help intelligence operations. In the case of the Americas, for instance, intelligence activities have regularly morphed into abuses and surveillance targeting opposition sectors as well as efforts to boost autonomy and restrict scrutiny by other agencies (Cate & Dempsey, 2017).

Although electronic evidence is critical for criminal investigations, the quantity of data that may be accessible can have various effects on privacy (Internet & Jurisdiction Policy Network, 2022). The proportionality principle should govern cooperation in this sense.

In the case of the American continent, except for the United States and Canada, most legal frameworks regulating data access are outdated (Internet & Jurisdiction Policy Network, 2022). Therefore, legislation should consider the diverse types of electronic evidence —such as subscriber information, transactional and traffic or access data, and content data— and adopt *ad hoc* access and protection procedures (Internet & Jurisdiction Policy Network, 2022).

At the international level, surveillance is defined as the interception of communications, regardless of whether the data is analysed or standardised (OAS, 2017). This surveillance includes the government's activities, including those carried out by other entities, such as service providers requested to provide access to data. (OAS, 2017).

At the international and regional level, surveillance violates people's privacy, hence the difficulty between protecting national security and people's rights (OAS, 2017).

In the overall EU digital rights picture, there are three major concerns 1) the debate around automatic filtering, 2) diversity of approaches in specific areas, and 3) concerns about Europol capabilities.

On the first point, the sentence of 26 April 2022 on the *Copyright Directive* authorises the use of automatic filters to protect copyright. Still, it does not set parameters to help platforms decide when it is acceptable to block content (Schmon et al., 2022).

Regarding the second point, despite the EU's joint vision, diverse approaches could conflict with each other, as evidenced by NetzDG in Germany and hate speech regulations in France (Barata Mir, 2020).

In terms of Europol's capacities, on 27 July 2022, EDPS issued a press release on the publication of the amended Europol Regulation in the EU Official Journal (EDPS, 2022a). The EDPS considers the adjustments to weaken data protection and do not ensure adequate supervision due to the extension of the mandate (EDPS, 2022a). Among the most worrying changes is the increase in the amount of data processed by the agency —even if it is unrelated to any criminal activity— and the inclusion of retroactive authorisation (EDPS, 2022a).

During the EDPS 2022 conference, it was emphasised that the citizenry must be made more aware of the bodies and rules available to protect their data (EDPS, 2022a). In addition, the conference emphasised the importance of broadening the academic debate beyond commercial surveillance and including that conducted by intelligence agencies. Fielder (2022) stressed the need to examine the technologies states use for surveillance purposes, the role of exceptions in legislation, and the long-term impact this situation will have on democracy (Fielder, 2022)

Transparency, clarification of responsibilities and dissemination of measures to protect citizens against possible abuse is necessary for

both regions. In the particular case of the European Union, it is needed that an organisation/body supervises intelligence agencies' activities when requesting personal data from ISPs, to safeguard the principle of proportionality.

Whereas this challenge is substantially more severe on the American continent, it requires the establishment of rules, responsible entities, transparency, the effective application of the law in practice, and collaboration for capacity building. The obstacles could also be mitigated by creating specialised bodies for internet governance, data protection and digital rights. Additionally, dialogue with ICANN, the ITU, ISPs, OAS officials, and national governments would undoubtedly enhance the digital rights situation.

Conclusion

Throughout this document, the state of digital rights and their protection by Internet Service Providers have been examined. As a result, it has become clear how digital rights regulation interacts with other laws governing e-commerce, copyright, national security, broadcasting regulation, and net neutrality, highlighting the complexity of the situation that ISPs, governments, and citizens face today. The preceding emphasises the interconnectedness and indivisibility of human rights, which are now exercised in the new context.

The situation is perceived differently by the European Union and the Organisation of American States, despite sharing common ground on specific topics. The findings are concentrated on three dimensions to answer the research questions: 1) the parties engaged and how they safeguard digital rights, 2) the rights that are infringed upon, and 3) the way both actors are promoting digital rights.

Mechanisms and actors involved in defence of digital rights

The European Union has a mostly uniform perspective, but with differences in specific topics such as combating hate speech. The EU has defined actors and regulations that enable the exercise and defence of digital rights in diverse dimensions. However, conversation on the limitations of security and intelligence organisations is required.

In the case of the OAS, the regional governments adhere to the *Inter-American Declaration of Human Rights*. In general terms, digital rights protection in the Americas is fragmented, despite OAS principles and recommendations and the binding nature of the court's judgements.

Particularly alarming is the lack of effective collaboration mechanisms, the variability of approaches to liability regimes, and the request for

adopting specific rules as a prerequisite to developing economic associations.

The above is primarily due to legislative asymmetries, the status of internet governance in the various nations, the lack of trust amongst members, the local complexities of economic development and security priorities, and the lack of technological knowledge on the matter. Nevertheless, this should not be a factor hindering progress on internet governance but rather a motivation for establishing collaboration structures.

Most affected digital rights

Specific rights in both regions are compromised in favour of copyright protection and national security concerns. In the case of the European Union, there are concerns over the scope of intelligence services monitoring and the quantity and variety of data Europol nowadays has access to. Moreover, it is unclear how certain groups would be safeguarded against this surveillance. These demographic segments, also known as vulnerable data subjects, could be subjected to a form of digital criminalisation and marginalisation.

On the ISP side, there are also risks since they are now subject to regulations such as those preventing online hate speech and terrorism. Faced with increasing demands from regulatory authorities, ISPs may implement automated systems concerned with being labelled as offenders. This final point is particularly pressing, since the employment of automated filters, while effective for copyright protection, is unquestionably a potential threat to freedom of speech and the right to information.

For the OAS and the region as a whole, the rights to freedom of speech, information, and privacy have emerged as a legacy of the battle against

military repression, particularly in Latin America, and as defining characteristics of a democratic state in the United States and Canada. Consequently, they are the most protected and promoted rights.

However, the OAS's limited scope and the region's complexities give rise to cases of abuse such as surveillance, privacy violations, and attacks on freedom of expression, not only in cases such as Venezuela but also in all nations that used spying tools such as Pegasus to monitor opposition and activists. This reality demands a robust structure for protecting digital rights and developing technological and legal capabilities, involving not just the OAS but also the ITU, and WIPO, among others.

Mechanisms for promoting digital rights

Digital rights in the European Union are promoted via the efforts of institutions such as LIBE and EDPS. Considering the evolution and direction of EU legislation, the protection of intellectual property and other interests, such as national security, appear to take precedence over digital rights. As seen in the previous analysis, economic interests drove the establishment of rules and institutions.

Nevertheless, digital rights are nowadays promoted through laws protecting personal data and net neutrality, a discussion that has evolved significantly over the past several years. It is crucial to draw attention to the LIBE and EDPS efforts since they are tasked with defending digital rights against interests and bodies devoted to preserving diverse priorities.

As indicated previously, in the Americas, particular importance is given to freedom of expression, access to information, and privacy due to the long road these rights had to walk to build democracy in the region.

These rights are promoted through declarations, recommendations, and calls for openness and transparency.

However, the OAS should transcend the debate and advocate for democratic internet governance among its member states, emphasising technical capacity building and regional expertise. In this regard, including a body specialised in digital rights within the Inter-American Court of Human Rights could be beneficial.

In general, both regions have three distinctive features:

1) Commercial interests as the primary engine for developing legislative mechanisms on digital activities, which unquestionably left digital rights behind. These two interests, —commercial vs human rights—, remain in constant conflict today in dimensions such as the protection of copyrights.

2) The intelligence agencies' competencies in terms of access to data and ISPs' cooperation with them are unknown in both the OAS and the EU. There is no possibility of accountability in the OAS owing to the lack of a regional framework. Thus, it is up to each government —and their commitment to democracy— the activities they allow under this modality.

For its part, the EU can benefit from the publication of annual transparency reports detailing the number of data requests by governments; this would provide an overview of the status of democracy on the internet.

3) ISPs are noticeably absent from forums and debates in both regions. ISP demands and concerns must be heard, and their capacities and understanding of human rights must be enhanced. There is also a need to develop safeguards against state-imposed obligations and offer

comprehensive reinforcement to equalise the weight of responsibilities that now rest on the shoulders.

As a result, the hypothesis regarding the involvement of ISPs and the predominance of copyright and national security priorities over digital rights is validated. However, in contrast to the hypothesis, the role of ISPs in data protection is determined not only by the nature of the internet but also by the economic and political value of personal data.

Internet Service Providers have a long way to go in digital rights protection, as they are crucial for internet functioning, and this is unlikely to change during the next several years. ISP must perform tasks such as removing potentially terrorist content, hate speech, and other activities that may impact digital rights, despite being mainly commercial actors.

This dissertation advocates for developing a new perspective on liability regimes —based on a people-centred view— which also prioritises the equitable distribution of responsibilities and the preservation of human rights.

Prospects demand constant reflection, continuous updating as the technology itself advances, and, most importantly, close coordination between Internet Service Providers, governments, civil organisations, and citizens to safeguard the status of human rights and democracy on the internet.

Bibliography

Adtran. (2021). Telecom Policy and Regulatory Landscape in the European Union. Adtran. https://www.adtran.com/media/amasty/amfile/attach/dLyW44VKqi8v17JXTTkJUBvHGAbOFPnV.pdf

Article 19. (2003). *The Johannesburg Principles: Overview and Implementation*. https://www.article19.org/data/files/pdfs/publications/jo-burg-principles-overview.pdf

Article 19. (2013). *Internet intermediaries: Dilemma of Liability*. https://www.article19.org/data/files/Intermediaries_ENGLISH.pdf

Article 19. (2018). *Side-stepping rights: Regulating speech by contract*. https://www.article19.org/wp-content/uploads/2018/06/Regulating-speech-by-contract-WEB-v2.pdf

Association for Progressive Communications (APC). (2006). APC Internet Rights Charter. *GenderIT.Org.* https://genderit.org/resources/apc-internet-rights-charter

Babinet, G. (2018). The End of Nation States? Part 1: Technology-Induced Sovereignty Transfers. Institut Montaigne. https://www.institutmontaigne.org/en/blog/end-nation-states-part-1-technology-induced-sovereignty-transfers

Banco Interamericano de Desarrollo (BID). (2020). *Resumen explicativo del estudio Responsabilidad de intermediarios de Internet en América Latina: Hacia una regulación inteligente de la economía digital" elaborado por el CETyS*. Asociación Latinoamericana de

Internet. https://alai.lat/wp-content/uploads/2020/12/Resumen-explicativo-Estudio-Intermediarios.pdf

Barata Mir, J. (2020). *Responsabilidad de proveedores intermediarios*. https://alai.lat/wp-content/uploads/2020/03/Presentacio%cc%81n-Joan-Barata-11Marzo-Mexico.pptx.pdf

Barnett, K. (2019). How European telcos are monitoring our online activity. *Social Europe*. https://socialeurope.eu/european-telcos-monitoring-online

Barzilai-Nahon, K. (2006). Gatekeepers, Virtual Communities and the Gated: Multidimensional Tensions in Cyberspace. *International Journal of Communications Law & Policy*. https://ciaotest.cc.columbia.edu/olj/ijclp/ijclp_11/ijclp_11i.pdf

Barzilai-Nahon, K., & Neumann, S. (2005). *Gatekeeping in Networks: A Meta- Theoretical Framework for Exploring Information Control*. https://www.researchgate.net/publication/228876470_Gatekeeping_in_Networks_A_Meta-Theoretical_Framework_for_Exploring_Information_Control

Bayer, J. & Internet Society of New Zealand. & Victoria University of Wellington. Law Faculty. (2007). Liability of internet service providers for third party content. [Wellington, N.Z: Victoria University of Wellington, Faculty of Law

Birchall, S. (2018). Copyright crack down: the implications for Australian Internet service providers under a free trade agreement between Australia and the United States. *Computers and Law*, (*52)*, pp. 25–29. https://doi.org/10.3316/agispt.20033434

Body of European Regulators for Electronic Communications (BEREC). (2015). *Tasks and Mission.* https://berec.europa.eu/eng/berec_office/tasks_and_role

Body of European Regulators for Electronic Communications (BEREC). (2016). BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules. https://www.politico.eu/wp-content/uploads/2016/08/BERECREPORT.pdf

Botero Marino, C. (2013). *Freedom of expression and the Internet. Inter-American Commission on Human Rights. Office of the Special Rapporteur for Freedom of Expression.* http://www.oas.org/en/iachr/expression/docs/reports/2014_04_08_Internet_ENG%20_WEB.pdf

Boyle, J. (2007). Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors. In *Law and Society Approaches to Cyberspace,* (6), pp. 177-205. https://scholarship.law.duke.edu/faculty_scholarship/619/

Brignall, T. W. (1998). The Foucault Panopticon Model in Motion: The Internet as a Candidate for Corporate Abandon. Master's Theses. [Western Michigan University]. https://scholarworks.wmich.edu/masters_theses/4853

Bustos Frati, G., Palazzi, P. A., & Rivero, S. (2021). *Responsabilidad de intermediarios de internet en América Latina: Hacia una regulación inteligente de la economía digital*. Publications. Banco Interamericano de Desarrollo. https://publications.iadb.org/publications/spanish/document/Responsabilidad-de-intermediarios-de-internet-en-America-Latina-Hacia-una-regulacion-inteligente-de-la-economia-digital.pdf

Butler, R. J., & Lachow, I. (2012). *Multilateral Approaches for Improving Global Security in Cyberspace*. https://www.mitre.org/sites/default/files/pdf/12_3718.pdf

Buzatu, A. M. (2020). *Global cybersecurity and the private sector.* Routledge Handbooks Online. https://doi.org/10.4324/9781351038904-32

Califano, B. (2013). *Políticas de Internet; La neutralidad de la red y los desafíos para su regulación*. Eptic. https://e-tcs.org/wp-content/uploads/2017/03/Califano-2013-Pol%C3%ADticas-de-Internet-la-neutralidad-de-la-red-y-los-desaf%C3%ADos-para-su-regulaci%C3%B3n.pdf

Cardelli, L., Orgad, L., Shahaf, G., Shapiro, E., & Talmon, N. (2020). Digital Social Contracts: A Foundation for an Egalitarian and Just Digital Society. http://arxiv.org/abs/2005.06261

Carr, M. (2016). *Public-private partnerships in national cyber-security strategies*. The Royal Institute of International Affairs. https://www.chathamhouse.org/sites/default/files/publications/ia/INTA92_1_03_Carr.pdf

Carrapico, H., & Farrand, B. (2017). “Dialogue, partnership and empowerment for network and information security: the changing role of the private sector from objects of regulation to regulation shapers”. *Crime, Law and Social Change*, 67(3), pp. 245–263. https://doi.org/10.1007/s10611-016-9652-4

Cate, F. H., & Dempsey, J. X. (Eds.). (2017). *Bulk Collection: Systematic Government Access to Private-Sector Data*. Oxford University Press. https://doi.org/10.1093/oso/9780190685515.001.0001

Cavelty, M. D. (2015). Cyber-Security and Private Actors. In *Routledge Handbook of Private Security Studies* (pp. 89-99). Routledge.

Center for Democracy and Technology. (2012). Shielding the Messengers: Protecting Platforms for Expression and Innovation. *Center for Democracy and Technology*. https://cdt.org/insights/shielding-the-messengers-protecting-platforms-for-expression-and-innovation/

Centro Criptológico Nacional (CN-CERT). (2022). *OEA firma acuerdo sobre ciberseguridad.* https://www.ccn-cert.cni.es/ca/gestion-de-incidentes/lucia/23-noticias/568-oea-firma-acuerdo-sobre-seguridad-cibernetica.html

Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE). (n.d.). Se presentaron los Principios de Manila sobre responsabilidad de intermediarios. *Universidad de Palermo*. https://www.palermo.edu/cele/noticias/principios_manila.html

Chen, L. S. (2017). Internet Service Provider Copyright Infringement in Taiwan. In G. B. Dinwoodie (Ed.), *Secondary Liability of Internet Service Providers* (Vol. 25, pp. 339–359). Springer International Publishing. https://doi.org/10.1007/978-3-319-55030-5_14

Christou, G., & Simpson, S. (2011). The European Union, multilateralism and the global governance of the Internet. *Journal of European Public Policy*, *18*(2), pp. 241–257. https://doi.org/10.1080/13501763.2011.544505

Clemente, D. (2013). *Cyber Security and Global Interdependence: What Is Critical?* Chatman House. https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/0213pr_cyber.pdf

Comisión Económica para América Latina y el Caribe (CEPAL). (2020). *Elementos principales del informe sobre el estado de la jurisdicción de Internet en América Latina y el Caribe 2020*. Naciones Unidas. https://repositorio.cepal.org/bitstream/handle/11362/46061/1/S2000403_es.pdf

Comisión Europea. (2013). *Guía del ciudadano sobre las instituciones de la UE*. https://www.aragon.es/documents/20127/8642196/C%C3%B3mo+funciona+la+Uni%C3%B3n+Europea.pdf/1fa7961c-0d02-f4c0-27e2-2b2c71fba087?t=1565173799949

Comisión Europea. (2022). Preguntas y respuestas: Ley de Mercados Digitales: garantizar unos mercados digitales justos y abiertos. European Commission. https://ec.europa.eu/commission/presscorner/home/en

Cortés, C. (2012). *Vigilancia de la Red: ¿Qué significa monitorear y detectar contenidos en Internet?* Centro de Estudios en Libertad de Expresión y Acceso a la Información, CELE. https://www.palermo.edu/cele/pdf/El-deseo-de-observar-la-red.pdf

Cortés Castillo, C. (2017). *Las llaves del ama de llaves: la estrategia de los intermediarios en Internet y el impacto en el entorno digital*. Centro de Estudios en Libertad de Expresión y Acceso a la Información. https://e-tcs.org/wp-content/uploads/2017/03/Cort%C3%A9s-2014-Las-llaves-del-ama-de-llaves-la-estrategia-de-los-intermediarios-en-Internet-y-el-impacto-en-el-entorno-digital.pdf

Council of Europe. (2011). Declaration by the Committee of Ministers on Internet governance principles. https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cc2f6

Council of Europe. (2014). *Guide to Human Rigths for Internet Users*. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d5b31

Council of Europe. (2016). *Internet Governance - Council of Europe Strategy 2016-2019.* https://rm.coe.int/16806aafa9

Court of Justice of the European Union. (2020). *The Court interprets, for the first time, the EU regulation enshrining 'internet neutrality'. Press Release No 106/20*. https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-09/cp200106en.pdf

Coyer, K., & Higgott, R. (2020). *Sovereignty in a digital era*. Research Institute. https://doc-research.org/wp-content/uploads/2020/09/Sovereignty-in-a-digital-era_____.pdf

Da Silva, J. (2022). Cyber security and the Leviathan. *Computers & Security,* (116), p. 102674. https://doi.org/10.1016/j.cose.2022.102674

Daigle, B. (2021). *Data Protection Laws in Africa: A PanAfrican Survey and Noted Trends*. Journal of International Commerce and Economics. https://www.usitc.gov/publications/332/journals/jice_africa_data_protection_laws.pdf

De Beer, J., & Clemmer, C. D. (2009). Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries.

Jurimetrics, (49), p. 375. https://heinonline.org/HOL/Page?handle=hein.journals/juraba49&id=383&div=&collection=

Defraigne, P. (2022a). “Abridged history on Net Neutrality debate in Europe – 2009-2014”. [Unpublished document]

Defraigne, P. (2022b). “Net Neutrality: State of play in Europe”. [Unpublished document]

Departamento de Derecho Internacional (DDI) & Organización de Estados Americanos (OEA). (2022). *Protección de Datos Personales* . https://www.oas.org/es/sla/ddi/proteccion_datos_personales.asp

Economic Commission for Latin America and the Caribbean (ECLAC), Jurisdiction, I. &, & Policy Network (I&JPN). (2020). *Internet & Jurisdiction and ECLAC Regional Status Report 2020 (LC/TS.2020/141)*. United Nations. https://www.cepal.org/sites/default/files/publication/files/46421/S1901092_en.pdf

El Universal. (2019) ¿De qué trata el caso Odebrecht? https://www.eluniversal.com.mx/nacion/politica/de-que-trata-el-caso-odebrecht

Electronic Frontier Foundation (EFF), Centre for Internet and Society, Article 19, KIKANET, Derechos Digitales, Asociación por los Derechos Civiles, & Open Net. (2015). *The Manila Principles on Intermediary Liability Background Paper*. EFF. https://www.eff.org/sites/default/files/manila-principles-background-paper-0.99.pdf

Etzioni, A. (2011). Private Sector Neglects Cyber Security. *The National Interest*. https://nationalinterest.org/commentary/private-sector-neglects-cyber-security-6196

Etzioni, A. (2014). The Private Sector: A Reluctant Partner in Cybersecurity. *Georgetown Journal of International Affairs*, pp. 69–78. https://www.jstor.org/stable/43773650

EU-LAC. (2019). Organización de los Estados Americanos (OEA). *EU-LAC Foundation*. https://intranet.eulacfoundation.org/es/mapeo/organizaci%C3%B3n-de-los-estados-americanos-oea-0

European Commission. (2014). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Internet Policy and Governance Europe's role in shaping the future of Internet Governance [EUR-LEX]. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52014DC0072

European Commission. (2022a). Open Internet | Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/open-internet

European Commission. (2022b). e-Commerce Directive | Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/e-commerce-directive

European Court of Human Rights (ECHR). (2021). *European Convention on Human Rights*. Council of Europe. https://www.echr.coe.int/documents/convention_eng.pdf

European Data Protection Board (EDPB). (n.d.). *Legal Framework - Coordinated Supervision Committee*. https://edpb.europa.eu/csc

European Data Protection Supervisor (EDPS). (2022a). The future of data protection. Effective enforcement in the digital world. https://www.edpsconference2022.eu/en/press-media/media

European Data Protection Supervisor (EDPS). (2022b). *Amended Europol Regulation weakens data protection supervision*. https://edps.europa.eu/system/files/2022-06/EDPS-2022-16-Press%20Statement%20on%20Europol%20Amended%20Regulation_EN.pdf

European Dialogue on Internet Governance (EuroDIG). (n.d.). More than just a conference. https://www.eurodig.org/

European Internet Foundation. (2009). *The Digital World in 2025*. European Internet Foundation. https://www.internetforum.eu/index.php?option=com_content&view=article&id=41

European Parliament. (2018). *Liability of Online Service Providers for Copyrighted Content – Regulatory Action Needed?* https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614207/IPOL_IDA(2017)614207_EN.pdf

European Parliament of the Council. (2000). Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). Official Journal of the European Communities. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN

European Parliamentary Research Service (EPRS). (2014). *Net neutrality in Europe*.

https://www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/140773/LDM_BRI(2014)140773_REV2_EN.pdf

European Union Agency for Cybersecurity (ENISA). (2022). Data Protection. ENISA. https://www.enisa.europa.eu/topics/data-protection

Fiedler, K., & McNamee, J. (n.d.). *Net Neutrality*. European Digital Rights. https://edri.org/files/EDRi_NetNeutrality.pdf

Fielder, A. (2022). *GDPR 25/30 What are we going to be discussing in a few years? The Future of data Protectio*n. [Video conference]. Effective enforcement in the digital world, Belgium. https://www.edpsconference2022.eu/en/press-media/media

Forden, E. (2015). *The Undersea Cable Boom in Sub-Saharan Africa*. USITC Executive Briefing on Trade. https://www.usitc.gov/publications/332/executive_briefings/forden_submarine_cables_june2015.pdf

Foucault, M. (1994). *Microfísica del poder.* Barcelona: Planeta-Agostini.

Foucault, M.(2014). *Vigilar y castigar*. Siglo XXI Editores: México.

Froncek, A., Canabarro, D. R., & Côrte Real, P. (2020). Mapeo de la responsabilidad de intermediarios en América Latina. Internet Society. https://www.internetsociety.org/es/blog/2020/08/mapeo-de-la-responsabilidad-de-intermediarios-en-america-latina/

Fundación Carolina. (2018). *Comunicación conjunta al Parlamento Europeo y al Consejo La Unión Europea, América Latina y el Caribe: aunar fuerzas para un futuro común*. https://www.fundacioncarolina.es/wp-

content/uploads/2019/06/UE-Comunicacio%CC%81n-conjunta-UE-ALC-2019-2.pdf

Furtak, F. T. (2015). Integration in Regional Organisations? A Comparison of EU, AU, OAS, and ASEAN. *Journal of Civil & Legal Sciences*, 04 (02), p. 2169-0170 https://doi.org/10.4172/2169-0170.1000146

Garrett, T., Setenareski, L. E., Peres, L. M., Bona, L. C. E., & Duarte Jr, E. P. (2022). A survey of Network Neutrality regulations worldwide. *Computer Law & Security Review*, (*44*). https://doi.org/10.1016/j.clsr.2022.105654

Global Intellectual Property Center (GIPC). (2017). The roots of Innovation. U.S. Chamber International IP Index (p. 148). http://www.theglobalipcenter.com/wp-content/uploads/2017/02/GIPC_IP_Index_2017_Report.pdf

Goldsmith, J., & Wu, T. (2006). Visions of a Post–Territorial Order. In J. Goldsmith & T. Wu, *Who Controls the Internet?* Oxford University Press. https://doi.org/10.1093/oso/9780195152661.003.0006

Guadamuz, A. (2001). Habeas Data vs the European Data Protection Directive. *Electronic Law Journals*. https://warwick.ac.uk/fac/soc/law/elj/jilt/2001_3/guadamuz/

Hadfield, D. (2017). Is the Panopticon a Useful Concept for Understanding Digital Surveillance? Thesis for: War Studies. https://www.researchgate.net/publication/322147602_Is_the_Panopticon_a_Useful_Concept_for_Understanding_Digital_Surveillance

Hare, F. B. (2009). Private Sector Contributions to National Cyber Security: A Preliminary Analysis. *Journal of Homeland Security*

and Emergency Management, 6(1). https://doi.org/10.2202/1547-7355.1426

Harknett, R. J., & Stever, J. A. (2009). The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen. *Journal of Homeland Security and Emergency Management*, 6(1). https://doi.org/10.2202/1547-7355.1649

Hathaway, M. E., & Savage, J. E. (2012). *Stewardship of Cyberspace*. University of Toronto. https://www.belfercenter.org/sites/default/files/legacy/files/cyber dialogue2012_hathaway-savage.pdf

Hiller, J. S., & Russell, R. S. (2013). The challenge and imperative of private sector cybersecurity: An international comparison. *Computer Law & Security Review,* 29(3), pp. 236–245. https://doi.org/10.1016/j.clsr.2013.03.003

Hobbes, T. (1997). *Leviatán.* México: Ediciones Gernika.

Hong, X., & Li, F. (2011). Analysis on Tort Liability of Internet Service Providers. In M. Zhou & H. Tan (Eds.), *Advances in Computer Science and Education Applications,* (202), pp. 475–480. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-22456-0_68

Horten, M. (*n.d.*). Net Neutrality. *IPIntegrity*. http://www.iptegrity.com/index.php/telecoms-package/net-neutrality

IEEE. (2017). Three Reasons Why Latin America is Under Cyber Attack. *IEEE Innovation at Work*. https://innovationatwork.ieee.org/latin-america-is-under-cyber-attack/

Inter-American Commission on Human Rights (IACHR). (2009). *Citizen Security and Human Rights*. http://www.cidh.org/countryrep/seguridad.eng/CitizenSecurity.V.a.htm

International Network of Privacy and Law Professionals (INPLP). (2018). A brief history of data protection: How did it all start? International Network of Privacy Law Professionals. https://inplp.com/latest-news/article/a-brief-history-of-data-protection-how-did-it-all-start/

International Telecommunication Union (ITU). (2022). European Union Agency for Network and Information Security. ITU. https://www.itu.int:443/en/ITU-D/Cybersecurity/Pages/Global-Partners/european-union-agency-network-information-security.aspx

Internet & Jurisdiction Policy Network. (2022). *FRAMING BRIEF: CATEGORIES OF ELECTRONIC EVIDENCES.* https://www.internetjurisdiction.net/uploads/pdfs/Data-Jurisdiction-Outcome-Framing-Brief-on-Electronic-Evidence.pdf

Intersoft Consulting. (n.d.). Privacy by Design. *General Data Protection Regulation (GDPR)*. https://gdpr-info.eu/issues/privacy-by-design/

Karsten, A. (2013). An introductory guide to internet governance: The European Union's work on internet governance. *Youth Policy*. https://www.youthpolicy.org/blog/internet-governance/european-union-internet-governance/

Katz, J. (1997). Birth of a Digital Nation. *Wired.* https://www.wired.com/1997/04/netizen-3/

Keller, C.I. (2019) *Exception and Harmonization: Three Theoretical Debates on Internet Regulation.* HIIG Discussion Paper Series, 2020 (02). http://dx.doi.org/10.2139/ssrn.3572763

Kelly, A. M. (n.d.). Section 230 of the CDA and Website Immunity [HG.ORG]. *The Kelly Law Firm, LLC*. https://www.hg.org/legal-articles/section-230-of-the-cda-and-website-immunity-20450

Kostopoulos, L. (2021). De facto shared sovereignty and the rise of non-state statecraft: Imperatives for nation-states. Observer Research Foundation. https://www.orfonline.org/expert-speak/de-facto-shared-sovereignty-and-the-rise-of-non-state-statecraft/

Lachow, I. (2016). The Private Sector Role in Offensive Cyber Operations: Benefits, Issues and Challenges. https://papers.ssrn.com/abstract=2836201

Laidlaw, E. B. (2012). Internet Gatekeepers, Human Rights and Corporate Social Responsibilities. PhD Thesis. [London School of Economics and Political Science]. https://core.ac.uk/download/pdf/4187775.pdf

Lesiak, M. (2009). A Comparative Analysis of The Liability of Internet Service Providers in The Context of Copyright Ingfingement in The U.S., European Union and Poland. *Masaryk University Journal of Law and Technology,* 3(2), pp. 279–292. https://journals.muni.cz/mujlt/article/view/2541

Levite, A., Kannry, S., & Hoffman, S. (2018). Addressing the Private Sector Cybersecurity Predicament: The Indispensable Role of Insurance. *Carnegie Endowment for International Peace.* https://carnegieendowment.org/2018/11/07/addressing-private-

sector-cybersecurity-predicament-indispensable-role-of-insurance-pub-77622

Liaropoulos, A. (2020). A Social Contract for Cyberspace. *Journal of Information Warfare*, 19(2), pp. 1–11. https://www.jstor.org/stable/27033617

Libicki, M. C. (2007). *Conquest in cyberspace: national security and information warfare*. Cambridge University Press.

Locke, J. (2010). *Two treatises of government* (Law Book Exchange edition). Lawbook Exchange, LTD.

Loewe, M., Zintl, T., & Houdret, A. (2021). The social contract as a tool of analysis: Introduction to the special issue on “Framing the evolution of new social contracts in Middle Eastern and North African countries”. *World Development*, (145), pp. 104982. https://doi.org/10.1016/j.worlddev.2020.104982

Lopez, A. [Alberto Lopez TECH TIPS]. (2021). ¿Cómo se Accede a INTERNET?►¿Qué es y Cómo funciona un Proveedor de Acceso a Internet (ISP)? [Video]. YouTube. https://www.youtube.com/watch?v=fwwZGO5Kvms

LSE IDEAS. (2018). A Digital Geneva Convention? The Role of the Private Sector in Cybersecurity. Medium. https://lseideas.medium.com/a-digital-geneva-convention-the-role-of-the-private-sector-in-cybersecurity-cd96ecd70622 \

MacKinnon, R. (2013). *Consent of the networked: the worldwide struggle for Internet freedom* (Paperback edition). Basic Books.

Madiega, T. (2020). *Reform of the EU liability regime for online intermediaries.* European Parliamentary Research Service.

https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/649404/EPRS_IDA(2020)649404_EN.pdf

Malaja, P. (2014). *The Liability of Internet Service Providers for Copyright Infringements: exception to copyright protection derived from freedom of expression*. Master Thesis. [Lund University]. https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=4580420&fileOId=4580421

Manila Principles on Intermediary Liability. (2015). https://www.eff.org/files/2015/10/31/manila_principles_1.0.pdf

Márquez, J. J. A. (2018). El principio de neutralidad en Internet. Una aportación a la libertad de comunicación en Internet desde el pensamiento de Francisco de Vitoria. *Estudios de Deusto*, *66*(2), pp. 71–103. https://doi.org/10.18543/ed-66(2)-2018pp71-103

Marsili, L. (2019). The rise of corporate nations. https://www.aljazeera.com/opinions/2019/7/19/the-rise-of-corporate-nations

Martin, C. D. (2013). The internet as a reverse panopticon. *ACM Inroads*, *4*(1), pp. 8–9. https://doi.org/10.1145/2432596.2432599

Marsden, C. T. (2012). Neutralidad de la Red: Historia, regulación y futuro. *IDP. Revista de Internet, Derecho y Política*, (13), pp. 24–43. https://www.redalyc.org/articulo.oa?id=78824460004

Marusic, B. (2016). Gate Keeper or Trespasser? EU ISP Liability Regime and its Privacy Implications. NIR: Nordiskt Immateriellt

Rättsskydd, (1), pp. 4–17. http://urn.kb.se/resolve?urn=urn:nbn:se:su:diva-134477

Master Internet and Computer. (2015). Definition, Role, Function Internet Service Provider. *Internet and Computer*. https://diarycomputer.blogspot.com/2015/01/definition-role-function-internet.html

McMullan, T. (2015). What does the panopticon mean in the age of digital surveillance? *The Guardian*. https://www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham

Mee, P., & Chandrasekhar, C. (2021). Trusted Internet Connections. CISA. World Economic Forum. https://www.cisa.gov/trusted-internet-connections

Meltzer, J. P. (2020). The Court of Justice of the European Union in Schrems II: The impact of GDPR on data flows and national security. *Brookings*. https://www.brookings.edu/research/the-court-of-justice-of-the-european-union-in-schrems-ii-the-impact-of-gdpr-on-data-flows-and-national-security/

Mishra, P., & Dutta, A. (2009). Striking a Balance between Liability of Internet Service Providers and Protection of Copyright over the Internet: A Need of the Hour. *JIPR, 14(4)*. http://nopr.niscair.res.in/handle/123456789/5215

Mittal, R. (2004). Online copyright infringement liability of Internet Service Providers. *Journal of the Indian Law Institute*, 46(2), pp. 288–321. https://www.jstor.org/stable/43951908

Morachimo, M. (2015). Principios de Manila: un estándar para las leyes sobre responsabilidad de intermediarios. *Hiperderecho*. https://hiperderecho.org/2015/04/principios-de-m

Morin-Desailly, C. (2014). Europe to the rescute of the Internet: Democratising Internet Governance relying upon a Europen Political and Industrial Ambition (N°696; A New Role and Strategy for the European Union in Internet Governance). SÉNAT. https://www.senat.fr/fileadmin/Fichiers/Images/commission/MCI_nouvelle_gouvernance_de_l_internet/EUROPE_TO_THE_RESCUE_OF_THE_INTERNET_english_summary.pdfanila-un-estandar-para-las-leyes-sobre-responsabilidad-de-intermediarios/

Morton, H. (2021). *Broadband 2020 Legislation. National Conference of State Legislatures.* https://www.ncsl.org/research/telecommunications-and-information-technology/broadband-2020-legislation.aspx

Municipalidad de Coronado. (2021). Organización de Estados Americanos. https://www.coromuni.go.cr/instituciones-gubernamentales/76-organizacion-de-estados-americanos.html

Naruse, K. K. (2018). Cyberspace and Foucault's Panopticon — The Rise of "Surveillance Society". Medium. https://medium.com/@kevinknaruse/cyberspace-and-foucaults-panopticon-the-rise-of-surveillance-society-61ec5846c409

O'Sullivan, K. (2014). Enforcing Copyright Online: Internet Service Provider Obligations and the European Charter of Fundamental Rights. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3124328

OAS, & OEA. (2009). OEA - Organización de los Estados Americanos: Democracia para la paz, la seguridad y el desarrollo https://www.oas.org/es/sla/ddi/tratados_multilaterales_interamericanos_A-41_carta_OEA.asp#Cap%C3%ADtulo%20I

Official Journal of the European Union. (2018). *REGULATION (EU) 2018/1727 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL - L 295/138*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1727&from=EN

Organización de Estados Americanos (OEA). (n.d.). CIDH: Seguimiento de Recomendaciones. https://www.oas.org/es/CIDH/jsForm/?File=/es/cidh/actividades/seguimiento/default.asp

Organización de Estados Americanos (OEA). (2009). Nuestra Estructura. https://www.oas.org/es/acerca/nuestra_estructura.asp

Organización de Estados Americanos (OEA). (2010). About e-Government. http://portal.oas.org/Portal/Sector/SAP/DepartamentoparalaGesti%C3%B3nP%C3%BAblicaEfectiva/NPA/Whatwedo/tabid/1814/Default.aspx

Organización de Estados Americanos (OEA). (2013a). Declaración Conjunta sobre programas de vigilancia y su impacto en la libertad de expresión https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=926&IID=2

Organización de Estados Americanos (OEA). (2013b). e-Gobierno, Gobernabilidad y Gobernanza.

http://portal.oas.org/LinkClick.aspx?fileticket=etN1Un2nMlU%3D&tabid=1729

Organización de Estados Americanos (OEA). (2015). Secretario de Seguridad Multidimensional de la OEA presenta políticas de ciberseguridad en Foro de Davos. OEA - Organización de los Estados Americanos. https://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-012/15

Organización de Estados Americanos (OEA) (2019). *Insumos de la Relatoría Especial para la Libertad de Expresión de la CIDH para el Informe sobre "Nuevas tecnologías, incluidas las tecnologías de la información y las comunicaciones, y su impacto en la promoción y protección de los derechos humanos en el contexto de las protestas"*. Comisión Interamericana de Derechos Humanos. https://www.ohchr.org/sites/default/files/Documents/Issues/RuleOfLaw/PeacefulProtest/IOs/iachr-sr-freedom-of-expression.pdf

Organization for Economic Co-operation and Development (OECD). (2010). Workshop Summary "The role of internet intermediaries in advancing public policy objectives." https://www.oecd.org/digital/ieconomy/45997042.pdf

Organization for Security and Co-operation in Europe (OSCE). (2011). *Joint declaration on freedom of expression and the Internet*. https://www.osce.org/fom/78309

Organization of American States (OAS). (n.d.). Best Practices Forum of the Americas. http://portal.oas.org/Portal/Sector/SAP/DptodeModernizaci%C3

%B3ndelEstadoyGobernabilidad/NPA/BestPracticesForumoftheAmericas/tabid/1168/language/en-US/default.aspx

Organization of American States (OAS). (2009a). Joint Declarations. https://www.oas.org/en/iachr/expression/basic_documents/declarations.asp

Organization of American States (OAS). (2009b). Press Release R50/11 - Freedom of Expression Rapporteurs Issue Joint Declaration Concerning the Internet. https://www.oas.org/en/iachr/expression/showarticle.asp?artID=848

Organization of American States (OAS). (2017). *Standards for a free, open, and inclusive internet.* http://www.oas.org/en/iachr/expression/docs/publications/internet_2016_eng.pdf

Organization of American States (OAS). (2022). *Updated Principles on Privacy and Personal Data Protection*. https://www.oas.org/en/sla/iajc/docs/Publication_Updated_Principles_on_Privacy_and_Protection_of_Personal_Data_2021.pdf

Oxford Pro Bono Publico (OPBP). (2021). *Regulation of Digital Media and Intermediaries*. University of Oxford. https://www.law.ox.ac.uk/sites/files/oxlaw/opbp_report-_regulation_of_digital_media_and_intermediaries.pdf

Parlamento Europeo. (n.d.). Poderes legislativos. https://www.europarl.europa.eu/about-parliament/es/powers-and-procedures/legislative-powers

Parliamentary Assembly. (2019). *Internet governance and human rights. Council of Europe.*

https://www.ebu.ch/files/live/sites/ebu/files/News/2019/01/Herkel%20REP%20-%20ENG%20-%20IG%20and%20Human%20Rights.pdf

Paynter, H., & Foreman, R. (2019). Liability of Internet Service Providers for Copyright Infringement. *The University of New South Wales Law Journal*, *21*(2), pp. 578–592. https://doi.org/10.3316/informit.108201071309533

Perritt, H. (1998). The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance. I*ndiana Journal of Global Legal Studies*, 5(2), p. 423. https://www.repository.law.indiana.edu/ijgls/vol5/iss2/4

Peruzzotti, M. (2020). El caso Schrems II y sus implicancias en la región. https://iapp.org/news/a/el-caso-schrems-ii-y-sus-implicancias-en-la-region/

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, 9(4). https://doi.org/10.14763/2020.4.1532

Portal de Administración Electrónica. (2022). PAe - El Consejo Europeo aprueba la Ley de Gobernanza de Datos. https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio2022/Mayo/Noticia-2022-05-19-El-Consejo-Europeo-aprueba-la-Ley-de-Gobernanza-de-Datos.html

Riley, M. C., & Scott, B. (2009). Deep Packet Inspection: The end of the Internet as we know it? *Freepress*. https://www.wired.com/images_blogs/threatlevel/files/dpi.pdf

Rocca, A. V. (2008). Zygmunt Bauman: modernidad líquida y fragilidad humana. Nómadas. *Critical Journal of Social and Juridical*

Sciences, 19(3), pp. 309–316. https://revistas.ucm.es/index.php/NOMA/article/view/NOMA0808320309A

Romero, T. L. (2006). Internet service providers' liability for online copyright infringement: the us approach. *Vniversitas,* 112, pp. 193–214. https://www.redalyc.org/articulo.oa?id=82511207

Rowe, B., Wood, D., Reeves, D., & Braun, F. (2011). *The Role of Internet Service Providers in Cyber Security.* Institution for Homeland Security Solutions. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.473.2323&rep=rep1&type=pdf

Sassen, S. (1999). The Impact of the Internet on Sovereignty: Real and Unfounded Worries. *Nautilus Institute for Security and Sustainability*. https://nautilus.org/information-technology-and-tools/the-impact-of-the-internet-on-sovereignty-real-and-unfounded-worries/

Savin, A. (2017). Internet regulation in the European Union. In *EU Internet Law* (pp. 1–17). Elgaronline. https://www.elgaronline.com/view/9781784717957/10_chapter1.xhtml

Schmitt, M. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd ed.). Cambridge: Cambridge University Press. https://doi.org/10.1017/9781316822524

---------International human rights law. In *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (pp. 179-208). Cambridge: Cambridge University Press. doi:10.1017/9781316822524.012

Schmon, C., Lukáš, F., & Mcsherry, C. (2022). La Directiva sobre derechos de autor de la UE sigue siendo sobre filtros, pero el máximo tribunal de la UE limita su uso. *Electronic Frontier Foundation*. https://www.eff.org/es/deeplinks/2022/05/eus-copyright-directive-still-about-filters-eus-top-court-limits-its-use

Shalika, C. (2019). Online Copyright Infringement and the Liability of Internet Service Providers. *Social Science Research Network*. https://papers.ssrn.com/abstract=3464140

Shushaanth, S., & Prakash G, A. (2020). A Study on Copyright Infringement in Cyberspace with Special Reference to the Liability of the Internet Service Provider for Infringement. *International Journal of Pure and Applied Mathematics*, 119 (17), pp. 1503-1516. https://papers.ssrn.com/abstract=3553588

Statewatch. (2022). EU: International personal data transfers: Presidency seeks 'a coherent and ambitious European policy'. https://www.statewatch.org/news/2022/may/eu-international-personal-data-transfers-presidency-seeks-a-coherent-and-ambitious-european-policy/

Strange, S. (1996). *The Retreat of the State: The Diffusion of Power in the World Economy*. Cambridge University Press. https://doi.org/10.1017/CBO9780511559143

----------The declining authority of states. In *The Retreat of the State: The Diffusion of Power in the World Economy* (pp. 3–15). Cambridge University Press. https://doi.org/10.1017/CBO9780511559143.002

Strange, S., & Palan, R. (2015). *States and markets* (New edition). Bloomsbury Academic.

Stoycheff, E., Liu, J., Xu, K., & Wibowo, K. (2019). Privacy and the Panopticon: Online mass surveillance's deterrence and chilling effects. *New Media & Society*, *21*(3), pp. 602–619. https://doi.org/10.1177/1461444818801317

Skelton, T. L. (1998). Internet Copyright Infringement and Service Providers: The Case for a Negotiated Rulemaking Alternative. *San Diego Law Review*, (35), 219. https://heinonline.org/HOL/Page?handle=hein.journals/sanlr35&id=227&div=&collection=

The Center for Internet and Society. (2018). *WILMAP*. Stanford Law School. https://wilmap.stanford.edu/

The European Consumer Organisation. (2022). *BEREC Draft Updated Guidelines on the Implementation of the Open Internet Regulation*. European Union. https://www.beuc.eu/publications/beuc-x-2022-038_beuc_response_updated-berec_guidelines_oir.pdf

Thomson Reuters. (2022). EU-US Privacy Shield (GDPR). *Practical Law.* http://uk.practicallaw.thomsonreuters.com/w-014-8180?originationContext=document&transitionType=DocumentItem&contextData=(sc.Default)&firstPage=true

Tosza, S. (2021). Internet service providers as law enforcers and adjudicators. A public role of private actors. *Computer Law & Security Review* (*43)*. https://doi.org/10.1016/j.clsr.2021.105614

United Nations. (n.d.). Dynamic Coalition on Internet Rights and Principles (IRPC). *Internet Governance Forum.* https://www.intgovforum.org/multilingual/content/dynamic-coalition-on-internet-rights-and-principles-irpc

United Nations. (2012). What is Human Security? https://www.un.org/humansecurity/what-is-human-security/

Unión Europea. (n.d.). Historia de la UE. https://european-union.europa.eu/principles-countries-history/history-eu_es

Unni, V. K. (2001). Internet Service Provider's Liability for Copyright Infringement- How to Clear the Misty Indian Perspective. *Richmond Journal of Law & Technology*, 8(2), p. 13. https://scholarship.richmond.edu/jolt/vol8/iss2/3

U.S. Copyright Office. (2017). *Introduction to the Third Edition of the Compendium of U.S. Copyright Office Practices*. https://www.copyright.gov/comp3/2017version/redlines/introduction.pdf

Van der Sloot, B. (2015). Welcome to the Jungle: The Liability of Internet Intermediaries for Privacy Violations in Europe. *JIPITEC*, 6(3). http://www.jipitec.eu/issues/jipitec-6-3-2015/4318

Vijay Mukane, R. (2016). Knowledge is Power: The Internet Panopticon as a Weapon against Terror. *E-International Relations*. https://www.e-ir.info/2016/05/19/knowledge-is-power-the-internet-panopticon-as-a-weapon-against-terror/

Villegas Carrasquilla, L. (2012). Personal data protection in Latin America: retention and processing of personal data in the Internet sphere. In *Hacia una Internet libre de censuraPropuestas para América Latina* (Eduardo Bertoni). https://www.palermo.edu/cele/pdf/english/Internet-Free-of-Censorship/05-Personal_data_protection_Latin_America_Villegas_Carrasquilla.pdf

Vranckaert, K. (2020). *ISP* Liability: How Censorship By Robots May Become the New Normal. *CITIP Blog*. https://www.law.kuleuven.be/citip/blog/isp-liability-how-censorship-by-robots-may-become-the-new-normal/

Wagner, B. (2013). Governing Internet Expression: The International and Transnational Politics of Freedom of Expression. PhD Thesis. [European University Institute]. https://www.academia.edu/5267237/Governing_Internet_Expression_The_International_and_Transnational_Politics_of_Freedom_of_Expression

Wan, K. S. (2011). Internet Service Providers' Vicarious Liability versus Regulation of Copyright Infringement in China. *University of Illinois Journal of Law, Technology & Policy*, pp. 375. https://heinonline.org/HOL/Page?handle=hein.journals/jltp2011&id=379&div=&collection=

Weber, R. H. (2010). Internet Service Provider Liability: The Swiss Perspective. *J. Intell. Prop. Info. Tech. & Elec. Com. L.,* (1), p.145. https://www.jipitec.eu/issues/jipitec-1-3-2010/2793/Weber_ISP_Ch.pdf

Wegbrait, P. (2014). Internet Service Provider liability for copyright infringement in Latin America. In D. Gervais & S. Frankel (Eds.), *The Evolution and Equilibrium of Copyright in the Digital Age* (pp. 180–202). Cambridge University Press. https://doi.org/10.1017/CBO9781107477179.013

Whitmore, S. E., Guest, L., & Oake, A. (2021). Media and communications: Risks of liability emerging for online platforms in Canada. *Insights. Torys LLP*. https://www.torys.com/our-latest-

thinking/publications/2021/11/risks-of-liability-emerging-for-online-platforms-in-canada

World Intellectual Property Organization (WIPO). (2002). WCT Enters into force. https://www.wipo.int/pressroom/en/prdocs/2002/wipo_pr_2002_304.html