GLOBAL PARTNERS DIGITAL

November 2016

Mapping the Cyber Policy Landscape: Chile

WRITTEN BY **J. CARLOS LARA AND PABLO VIOLLIER**

Global Partners Digital
Second Home
68 - 80 Hanbury Street
London
E1 5JL
+44 (0)203 818 3258
info@gp-digital.org
gp-digital.org

Global Partners & Associates Ltd
Registered in England and Wales

Designed by SoapBox
Typeset by Erwin Yin
Cover image adapted from David Nagy under Creative Commons Licence 2.0.
https://www.flickr.com/photos/ndave/

Company Nº 520 1603
VAT Nº 840 1912 54

GLOBAL PARTNERS DIGITAL

Mapping the Cyber Policy Landscape: Chile

WRITTEN BY J. CARLOS LARA AND PABLO VIOLLIER

gp-digital.org

CONTENTS

01

INTRODUCTION

According to estimates by the World Bank, over 72% of Chileans were internet users by the year 2014,[1] a much higher figure than the 65 % ITU estimate for the Americas (including developed countries like the United States and Canada) for 2016.[2] For a highly centralised developing country with a complicated geography and relative isolation from the rest of the South American continent, let alone the rest of the world, this is seen as a success in digital inclusion.

In theory, this level of internet penetration would correlate with certain trends in public policies – for example, legislative measures regarding issues like connectivity, digital entrepreneurship or content regulation, or a framework which acknowledges challenges arising from growing internet use. Even a quick glance at the Chilean policymaking landscape shows that this is not the case. There's little in the way of rules and regulations regarding the internet and its related issues, aside from a few disconnected initiatives which are in some aspect related to information and communications technologies.

Although there is a strong Chilean market for ICT services, its growth is mostly linked to general economic conditions – characterised by the dominance of large, mostly international players, and high connectivity costs. Recent policies by authorities such as the Undersecretariat of Telecommunications have made efforts to foster growth in places away from large urban centres, in order to close the gap between cities and rural areas, and between the highly connected capital Santiago and the most isolated cities and towns, while allowing strong market forces to compete for the provision of services in more densely populated areas.

There have been several normative initatives to regulate ICT development. Chile is notably one of the first countries to have enshrined into law both the net neutrality principle,[3] and exemptions from liability for copyright infringement in favour of internet intermediaries;[4] a progressive record. At the same time, it has a metadata retention mandate for local ISPs of up to one year;[5] a data protection law which, while one of the first in the region, allows the collection and broad use of personal information without consent;[6] and a law on cybercrime that dates back to 1993 and penalises hacking and other acts in extremely broad terms.[7] Efforts to substantively modify or replace the most questionable statutes have found little to no success in Congress. Over the last two decades, each successive government has launched a new "digital agenda" – typically a package of measures with variable links to ICTs. But with no centralised authority to guide these agendas, no continuity from one agenda to the next, and none of the urgency and focus necessary to realise their ambitious goals, progress has been slow.

However, a glimmer of hope can be seen in the second Bachelet administration's announcement of a National Cybersecurity Policy. Unlike previous processes, the

1. The World Bank, "InternetInternet users (per 100 people)", http://data.worldbank.org/indicator/IT.NET.USER.P2?locations=CL
2. International Telecommunications Union, "ICT Facts and Figures 2016", http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf
3. Law No. 20,453, 2010.
4. Law No. 20,435, 2010.
5. Article 222, Criminal Procedure Code.
6. Law No. 19,628, 1999.
7. Law No. 19.223, 1993.

comprehensiveness of the themes considered in its drafting - and the involvement of a very diverse group of actors - allowed for a broader discussion, aided also by an open public consultation on the Policy's guiding document.

The National Cybersecurity Policy process, still ongoing, includes a broad view of the involved topics, and a decidedly bigger opportunity for public participation. Yet the success of that process still cannot be declared. Whether a similar (or better) model for policymaking will be seen in Chile, or could be aspired to, is still pure speculation – in no small part, because of the variety of stakeholders relevant to the regulation of ICT policy issues. In the following pages we will identify these actors, and explore the current state of Chile's cyber policy landscape.

02

METHODOLOGY

The first step in our efforts to produce a map of relevant participants in Chile's policymaking processes, following Souter (2010), was to separate them into four different categories: government, private sector, internet technical and professional community, and civil society.[1] This categorisation might seem obvious, but in Chilean policymaking there is still a tendency to divide participating actors only by public and private sector. This is particularly troublesome since organised civil society (public interest non-governmental organisations and such) and the private sector have very different agendas in policymaking processes, as well very different interests and resources. Also, policymaking processes tend to equate the internet technical and professional community with civil society when they are not part of either government or the private sector. Even though civil society groups can (and arguably should) have a technical approach to cyber policy issues, the position the internet technical and professional community has in cyber policy issues remains qualitatively different to that of civil society.[2]

After categorising the participants in cyber policymaking processes by their nature, the next step was to separate them according to the layer of the internet in which they participate - using the simple three-layer model for ICT policy (Peña, 2013; Vera, 2014): physical, logical and content.

The latter categorisation is relevant, since it helps to assess if certain policymaking process infringe one of the two pillars of the layer separation principle. The first pillar relates to transparency. Layer-violating regulation may damage transparency, which can affect the costs of innovation (Colum and Chung, 2003); therefore, policymakers should not compromise the separation of layers when regulating the internet. The second pillar states the fact that regulations which affect different layers of the internet suffer from problems of overbreadth and underinclusion. Therefore, in regulating one layer, regulators should aim not to affect another at the same time (Colum and Chung, 2003). Using this categorisation and these principles, we can better understand the reach and scope of certain processes, as well as the level of participation of different actor types.

Finally, all relevant actors have been categorised according to twelve main issues related to cyber policymaking, as a means of showing which processes they have participated in, or may in the future. Though this list is under constant revision, it currently considers:

- Promotion of internet access and quality of connectivity;
- Education;
- Cybercrime;
- Cybersecurity;
- Copyright and access to knowledge;

1. Souter actually proposes five categories, including "Nation states", but since our research is focused on Chile, we have decided to use only four categories.
2. It is arguable that associations of users might constitute an altogether different category, but is is difficult to identify one in Chile with sufficient differentiation.

- Digital rights;
- Personal data protection;
- Domain name system;
- Open data and open government;
- Infrastructure;
- Net neutrality;
- Internet governance.

The process of information-collecting was conducted primarily using publicly available information, including data published under the duty of "active transparency" which public entities have. Since the enactment of Law No. 20,285, which enshrines the right to access public information, all acts and resolutions of public authorities are declared public, along with their legal basis and the documents related to them. The law enacts two obligations that guarantee the exercise of this right.

The active transparency duty[3] stipulates that public agencies must release, through their websites, all "spaces and mechanisms for civil participation" among other relevant information. This mechanism enabled us to scan all public agencies that have had a role in the elaboration or enactment of cyber policies. The "passive transparency" duty[4] is the version in Chilean law of the duty to respond to information requests, and requires all public agencies to provide access to any document or information requested by an individual, with the exception of cases expressly established by the same law. Annual reports released by relevant state agencies were also reviewed for further information.

Regarding the involvement of the private sector, civil society and the internet technical and professional community in past cyber policymaking processes, the active transparency duty also proved useful. Since most information regarding instances of civil participation is public (in varying degrees of detail), this allowed us to review all relevant actors that have participated in public consultation processes regarding cyber policy issues.

Another key source of information, though a more informal one, was internal knowledge. At Derechos Digitales, we've spent the last 11 years advocating from a public interest perspective on the cyber policy issues identified by this report, and have been actively engaged in policymaking processes at the national level. Chile is a small country with a limited amount of stakeholders - and so our involvement in past and present processes has allowed us to meet and hold dialogues with almost every relevant private sector, civil society and professional community actor at one point or another.

We have also established contact with representatives of all four categories of relevant actors to gather their views on the current state of cyber policymaking in Chile, with particular emphasis on the three latest and most relevant processes: Digital Agenda 2020,[5] the Civil Society Council for Data Protection[6] and the ongoing National Cybersecurity Policy consultation process.[7]

Certain public documents and past research proved particularly useful in mapping relevant participants in policymaking processes. For example, the released National Cybersecurity Policy draft[8] contained two annexes, one stating the regulations and institutions that intervene in Chilean cybersecurity, and the other providing an overview of key threats to national cybersecurity. We also benefited from other investigations by Derechos Digitales which have covered similar ground (Lara, Vera and Viollier, 2014; Viollier, 2016), with a somewhat less ambitious mapping of relevant actors relating to internet issues.

3. Article 7 j) , Law No. 20,285
4. Article 10, Law No. 20,285.
5. http://www.agendadigital.gob.cl
6. http://www.economia.gob.cl/consejo-de-la-sociedad-civil-de-proteccion-de-datos-personales
7. http://ciberseguridad.interior.gob.cl/consulta-ciudadana/
8. http://ciberseguridad.interior.gob.cl/media/2016/02/Borrador-Consulta-P%C3%BAblica-PNCS.pdf

As for the construction of the mapping's dataset, we used Internet Democracy Project's "Watchtower"[9,10] initiative as a reference point, but slightly modified it to accommodate the inclusion of non-governmental institutions.

Finally, in developing definitions and the framework for assessing a successful process of national cyber policymaking, we used Global Partners Digital's "Multistakeholder framework for national cyber policymaking processes" (GPD, 2016) series as a reference point.

9. https://internetinternetdemocracy.in/watchtower/

10. The Watchtower's dataset is available at: https://docs.google.com/spreadsheets/d/1t_7K7Asg92NXmt9EDxvrQFYdy1w7XWMsft2xJTRTo8M/edit#gid=0

03

PRELIMINARY FINDINGS

Our research conducted on public agencies through their active transparency duty, and the study of the three latest and most relevant processes (Digital Agenda 2020, Civil Society Council for Data Protection and the National Cybersecurity Policy), reveal some preliminary findings worth mentioning.

Jurisdiction over cyber policy matters is distributed among several government agencies, which in turn depend on different ministries without a clear role assignation, and without coordination when they may affect cyberspace. A symptom of this lack of institutional stability is that over the last few years, certain cyber policy issues have, at various times, come under the responsibility of different state agencies. When these changes in jurisdiction happen, a clear reason is rarely given.

A good example is the Undersecretariat of Digital Development. This used to be located in the Ministry of Transport and Telecommunications; then, for a few years it was part of the Ministry of Economy, Development and Tourism. This year, it became part of the Secretariat General of Government.[1]

In other cases, discerning which state agency is in charge of a certain policymaking process can be even more troublesome. Such is the case of the process regarding the drafting of a new personal data protection bill, which was at first conducted by the Minister of Economy, Development and Tourism. The process involved the creation of a multistakeholder group that worked on a draft of the bill; a public consultation process for commenting on the draft in parallel; and the inclusion of the data protection reform in the Digital Agenda 2020. Nevertheless, the process seemingly fell out of the influence of the Ministry in a highly turbulent few months, which saw the resignation of an Undersecretary of Economy while the draft bill underwent broad revisions by the Ministry of Finance. This sequence of events produced high levels of uncertainty regarding the future of the new Data Protection Law, especially since press statements by the Minister of Finance contradict content from the last publicly known draft in fundamental areas, including the very nature of the proposed data protection authority (Viollier, 2016).

An important related factor is the absence of a centralised government entity with a clear mandate over certain cyber policy issues. For instance, Chile still lacks a personal data protection authority in charge of enforcing Law No. 19,628, leaving individuals with no other choice than to go through the courts on their own. The Council for Transparency has jurisdiction over personal data processing in public entities, but lacks the authority to impose sanctions (Matus, 2013).

1. http://www.agendadigital.gob.cl/#/quienes-somos/secretaria#top-page

Even though the announcement of a National Cybersecurity Policy represents a major step forward in this area, it still depends on a transitory institution which has a mandate to elaborate a proposal, but not to implement it. The same can be said of the successive versions of the digital agenda. Every administration in the past two decades has released a different version of a digital agenda, yet to date none of them has resulted in a clear roadmap for long term public policy, and no evaluation has been carried out to measure each agenda's success. The current one ("Agenda Digital 2020") presents 60 measures in varying levels of detail, but the document does not include an executive structure for the implementation of those measures or an explanation as to why some measures are prioritised over others; nor do these measures have a responsible entity, or deadlines or evaluation mechanisms.[2] One of the reasons for this tendency is probably that these processes do not usually have a single entity in charge, but instead are commissioned by ad-hoc coordinating interministerial bodies without a clear mandate or authority to see through the implementation process, which makes it more difficult to make them accountable for the lack of implementation of the policy changes proposed.

In a different area, regarding the facilitation of the engagement of non-governmental entities in public policymaking processes, the enactment in the year 2011 of Law No. 20,500 on associations and citizen participation in public affairs presented a major breakthrough. Article 70 of the law states that "Each organ of the public administration must establish formal and specific modalities of participation for individuals and organization within the framework of its competence". Article 74 also states that "State administration bodies must establish civil society councils of an advisory nature, that must be formed in a diverse, representative and pluralist manner by members of non-profit associations that have a relation with the respective domain of competence of the body".

This has led to a proliferation of civil society councils in different state agencies, including three related to cyber policy issues.[3] Velasco (2016) found that 31 civil society councils were reported active as of the year 2016. Nevertheless, a closer look is necessary to assess if these bodies are fulfilling their intended purpose. Data shows that civil society councils are composed primarily of males (68%), and of a total of 214 council members, 30% are related to civil society organisations, 22% to NGOs and 20% to business associations (Velasco, 2016).

Public consultation processes have also been on the rise, with mixed results. The National Cybersecurity Policy public consultation was widely considered a clear, transparent process, open to newcomers, albeit with high barriers to entry. Previous data protection reform processes have had a more troublesome road. In 2011, during the previous administration, a public consultation process was conducted. But the results of this public consultation, paradoxically, were not released, and access was denied when requested, for the stated reason that it did not constitute "public information" under Law No. 20,285.[4] A new version of this public consultation, now under the current government, was conducted in 2014. Even though the public consultation process was conducted thoroughly, the whole process was later located in a different ministry as mentioned. And the final draft of the Digital Agenda 2020 – developed through a process which called for the participation of dozens of entities and groups – was not shared outside the Ministry of Economy before its publication.

Our mapping of internet technical and professional community actors found a handful of organisations, some of which are the Chilean chapters of international associations (ISSA and ISACA), which do not appear to be very active in the national forums. By contrast, the mapping of private sector shows that, even though the amount of associations is small, they include a great amount of companies and members (hundreds in the cases of ACTI and SCG). Our study of public consultation and cyber policy making processes show that these

2. See Ruiz, C., "Agenda Digital 2020: una vaga lista de deseos", Derechos Digitales, December 10th 2015, available at: https://derechosdigitales.org/9593/agenda-digital-2020-una-vaga-lista-de-deseos/
3. See the accompanying chart.
4. Derechos Digitales, "ONG Derechos Digitales recurre de Transparencia por consulta pública sobre Ley de Datos Personales", April 12 2012, available at: https://derechosdigitales.org/2658/ong-derechos-digitales-recurre-de-transparencia-por-consulta-publica-sobre-ley-de-datos-personales/

organisations are very active in participating in all of the forums in which they can defend their interests, including Congress and the executive.

Civil society, on the other hand, presents a rather different landscape. Ten main organisations were identified as active, focused mainly on issues relating to copyright and access to knowledge, open data and open government, and personal data protection. Even though this category has the second highest number of actors involved in cyber policymaking (after state actors), a closer look shows that only two of them have ten or more people employed full time (Derechos Digitales and Ciudadano Inteligente). Most of these organisations either depend on grants by foreign organisations, or depend on volunteer work, meaning their members have full-time employment elsewhere and only have their free time to work with these organisations.

Chile lacks a public policy regarding the financing of civil society organisations, which means the funding landscape is characterised by a shortage of projects and the small amount of money involved. Also, existing projects do not include remuneration for activities such as lectures, workshops and the like, seriously affecting the reach that civil society initiatives can achieve. Further research is necessary to assess the probable impact that the resource factor has on their participation in the national policymaking agenda.

Despite the ongoing tendency to carry out public consultation processes and create civil society councils, a trend that is well received by civil society organisations, the fact that these processes generally involve dozens of hours of long meetings and work without direct compensation, coupled with the difficulty of securing funding, has generated some discontent. This sensation is worsened when civil society groups invest hours of work in processes that never see the light of day, such as the data protection reform bill, or become involved in processes that are ultimately deemed to be a mere façade of public participation. Because of the resources and funding mechanisms they possess, this does not seem to impact public agencies and the private sector to the same extent. In short, it is unclear whether participation is encouraged under conditions of scarce resources and limited impact, bringing into question the value of current participation mechanism. More investigation is needed into this question.

Finally, as mentioned above, civil society organisations feel that the discourse used by government entities still emphasises the public/private dualism, with most of the policymaking processes still evoking the necessity of "public–private partnership" as a relationship between regulator and regulated entities. A shift of language is still required to install the multistakeholder approach in all cyber-related policymaking processes. The National Cybersecurity Policy draft is a step in the right direction (with consultations before and after the draft proposal), and it would be a positive development if other public agencies followed the example.

04

NEXT STEPS: TOWARDS A MODEL CYBER POLICYMAKING PROCESS

Exploring the Chilean cyber policy landscape in terms of relevant actors and participants of policymaking processes over the past several years also allows us to revisit these processes, and take a fresh look at their results. It also serves to acknowledge pending policymaking processes that have been hinted at in the past but do not have an expression in official initiatives.

A model for policymaking in Chile around topics related to ICTs and the internet will necessarily have to take into consideration some of the more idiosyncratic elements of the Chilean landscape, some of which were listed in the previous section. At the same time, feedback from different actors will still be needed to assess some of the gaps in knowledge or perspective that arise from gathering information from the point of view of a civil society stakeholder.

For some time Derechos Digitales has been discussing potential models for cyber policymaking processes, based on prior experience in certain processes. Nevertheless, further reflection on the key nodes for effective policymaking in this context will likely be necessary.

The National Cybersecurity Policy process offers an opportunity for this kind of reflection. As an ongoing process, it enables different stakeholders to study Chile's evolution regarding multistakeholder policymaking processes and potentially influence its outcomes.

As of the writing of this report (November 2016), the "Interministerial Cybersecurity Committee" is still analysing submissions to the first National Cybersecurity Policy draft,[1] and the final version of the document, which should address the comments submitted by all the participants, is scheduled to be published before the end of 2016.

Because of its promising start, high expectations have been placed on the outcome of this process. If the comments and input from stakeholders are not properly taken into account in the final version, it could further diminish trust in future cyber policy processes. Institutional challenges will also be a factor, since the Interministerial Cybersecurity Committee institutional structure is in itself transitory.

But if it succeeds, the National Cybersecurity Policy process may become a positive example for future cyber policymaking processes in Chile.

1. The submissions and comments from all participating actors can be found here: http://ciberseguridad.interior.gob.cl/consulta-ciudadana/

05

ACTOR MAPPING

Download the actor mapping chart here (xls file)

06

REFERENCES

Global Partners Digital, “Multistakeholder framework for national cyber policymaking processes”, at: http://www.gp-digital.org/series/multistakeholder-framework-for-national-cyber-policymaking-processes/

Lara, C., Vera, F and Viollier, P. (2014), “Estado de Internet en Chile: aspectos generales, regulación y actores relevantes”. Santiago: Derechos Digitales.

Matus, J. (2013), “Derecho de acceso a la información pública y protección de datos personales”, RCHDT vol. 2 n. 2. DOI 10.5354/0719-2584.2013.26959

Peña, P. (2013), “¿Cómo funciona Internet? Nodos críticos desde una perspectiva de los derechos”. Santiago: Derechos Digitales.

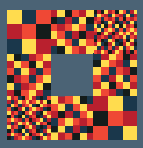
Solum, L. B. and Chung, M. (2003), “The Layers Principle: Internet Architecture and the Law”. U San Diego Public Law Research Paper No. 55. Available at SSRN: http://ssrn.com/abstract=416263

Souter, D. (2010), “Mapping Internet Public Policy: Notes on slide presentation to APC symposium on Networking Networks in Internet Public Policy”. APC, at: https://www.apc.org/en/system/files/APCMappingInternetPublicPolicy_Presentation.pdf

Velasco, P. (2016), “Sobre la conformación de los Consejos de la Sociedad Civil” (draft).

Vera, F. (2014), “Regulación internacional de Internet:una aproximación desde las capas de la red”, RCHDT vol. 3 n. 2. DOI 10.5354/0719-2584.2014.35396

Viollier, P. (2016), “El estado de la protección de datos personales en Chile: La ley, la agenda, la tecnología, los actores relevantes”, Santiago: Derechos Digitales (draft).



GLOBAL PARTNERS DIGITAL

Human rights in a connected world

GLOBAL PARTNERS DIGITAL
Second Home
68 - 80 Hanbury Street
London E1 5JL
+44 (0)20 3 818 3258
gp-digital.org