GISWatch 2017
SPECIAL EDITION

UNSHACKLING EXPRESSION:

A STUDY ON LAWS CRIMINALISING EXPRESSION ONLINE IN ASIA

Association for Progressive Communications (APC)

GISWatch 2017
SPECIAL EDITION

Unshackling expression: A study on laws criminalising expression online in Asia

APC

Coordinating committee
Gayatri Khandhadai (APC)
Pavitra Ramanujam (APC)
Geetha Hariharan

Project coordinator
Gayatri Khandhadai (APC)

Edition coordinator
Geetha Hariharan

Assistant editor, publication production
Lori Nordstrom (APC)

Graphic design
Monocromo
info@monocromo.com.uy
Phone: +598 2400 1685

Cover illustration
Ivana Kurniawati

Supported by the European Union under the Instrument for Democracy and Human Rights (EIDHR) and the Internet Policy Observatory (IPO)

Published by APC
2017

Printed in India

Global Information Society Watch 2017 | Special edition
Unshackling Expression: A study on laws criminalising expression online in Asia

ISBN 978-92-95102-86-6
APC Serial Number: APC-201711-CIPP-R-EN-DIGITAL-276

Disclaimer: The views expressed in GISWatch are not necessarily the views of APC or of its members

A methodology for mapping the emerging legal landscapes for human rights in the digitally networked sphere

By Jessica Dheere
SMEX
https://www.smex.org

The methodology used to conduct the research for Unshackling Expression is based on a methodology developed by SMEX. This chapter provides an overview of the methodology's development and use. For the purposes of our own research, the methodology, insofar as it related to the classification of laws into legal foundations, fundamental rights and freedoms, governance of online and networked spaces, sectoral laws and other laws, was especially helpful in defining the scope and limitations. In each country, these classifications were applied to understand the nature of laws affecting cyberspace, and more particularly, the laws criminalising online freedom of speech and expression. Thus, the entire concept of digital rights was not adapted for Unshackling Expression; we restricted our research to the right to freedom of opinion, speech and expression online, and more narrowly, to laws that criminalise this right. Towards this end, we adapted the legal classifications to identify the laws that affect freedom of speech online by way of criminalising such expression.

There are, of course, many ways in which governments restrict digital rights, including the right to freedom of opinion, speech and expression. Laws are merely one tool. However, laws form the primary legitimising tool to restrict digital rights. As Article 19 of the International Covenant on Civil and Political Rights (ICCPR) makes clear, any restriction on the right to freedom of expression must be grounded in law, and this law must be both enacted and made available to the public. Laws that criminalise speech online form a sub-category of laws that restrict digital rights, and comprise the subject of this report, Unshackling Expression.

Introduction: Why we need a methodology to identify laws affecting human rights in the online sphere

Why study laws that restrict digital rights?

Around the world, civic space is shrinking.[1] This contraction is in large part the result of attempts by governments to assert their sovereignty and regulate the internet and other aspects of the digitally networked sphere through legal controls. In many cases these controls aim to deal with legitimate challenges, such as certifying e-transactions, the theft of personally identifiable information, and other forms of internet-enabled crime, but often they are drafted from an uninformed or myopic perspective of how law, and thus rights, translate to the digital realm. In other cases, these controls consist of outdated legislation, such as analogue-era press and publications laws, clumsily interpreted for the digital sphere. In most cases, because the development and application of law to the digital realm is frequently ad hoc, it can be difficult for online rights advocates to conceptualise these frameworks, identify their weaknesses, analyse emerging trends, qualify their impact and, most important, push for reform.

In 2013, as the optimism of the so-called Arab Spring began to wane, governments in the Middle East and North Africa (MENA) reacted to the uprisings and revolutions by cutting off NGO funding, upping surveillance, and detaining and arresting activists and journalists under false pretences – frequently under cover of vague statutes and arbitrarily applied law.

To gain a better understanding of this emerging minefield of red lines, SMEX launched two separate but concurrent inquiries into the emerging legal framework for online expression and press freedom. The first, a pilot research initiative conceived

[1] Bustos, C. (2017, 17 April). The Shrinking of Civic Spaces: What is Happening and What Can We Do? *Dejusticia*. https://www.dejusticia.org/en/the-shrinking-of-civic-spaces-what-is-happening-and-what-can-we-do

and executed with support from Hivos' now-defunct iGmena programme,[2] involved collecting legislation related to the digital sphere in six Arab countries (Egypt, Iraq, Jordan, Tunisia, Lebanon and Syria); the second, a report commissioned by the Doha Centre for Media Freedom, prompted a broad review of existing documentation of the legal and policy framework for online media in all 22 countries of the Arab League. The exchange between these two projects yielded the first iteration of both a methodology for collecting, categorising and analysing digital rights-related legislation, and a solid baseline of data on the emerging legal landscape for digital rights in the Arab region, which we now call the Arab Digital Rights Datasets (ADRD).

A public version of the ADRD[3] has resided on the online data visualisation platform Silk[4] since 2015.[5] It contains 142 individual laws from 20 Arab states, organised by country and keywords, many of them accompanied by translations to English or French. It is the product of the work of more than a dozen contributors, including lawyers, journalists, activists and technologists from the countries in question, who through an inductive research process[6] gathered laws that they considered to affect digital rights. These included laws that:

- Establish or limit freedom of expression, freedom to assemble, the right to privacy, the right to access information and press freedom.
- Criminalise acts of speech, including over electronic channels.
- Regulate the industries that operate electronic communications channels.
- Govern content production and sharing, such as copyright and intellectual property laws.
- Govern electronic commerce, such as etransaction and esignature laws.
- Empower state surveillance.
- Have been cited in digital rights-related cases.

Working with a clearly delineated methodology

By cataloguing national-level legislation affecting the online sphere, SMEX aimed to assist not only activists but also human rights lawyers, judges, law and policy makers, researchers and journalists to build credible, compelling narratives for the protection and promotion of human rights in the digitally networked sphere. In the information collected and the patterns it could help us identify, we saw numerous opportunities to advance a common understanding of emerging legal frameworks for the online realm. Free and open access to such data would help human rights lawyers locate relevant articles and guiding jurisprudence. Digital rights legal researchers or journalists could access essential texts or other data liberated from PDFs and available outside legal database paywalls. Advocates, faced with a deluge of assaults on digital rights, might discover trends or pressure points that would help them better allocate limited campaign resources. The data could also be used to brief public officials and representatives who are committed to rights but struggle to keep pace with technology's implications for the societies we live in.

Initially released in September 2015 at an Internet Policy Observatory research methods workshop in Istanbul, the datasets found an early following among researchers at civil society organisations that document and defend digital rights. In April 2016, the Electronic Frontier Foundation (EFF) released *The Crime of Speech*,[7] a report by Wafa ben Hassine, who relied heavily on the dataset. Soon afterward, the Association for Progressive Communications (APC) published *Digital rights advocacy in the Arab world and the Universal Periodic Review*,[8] also by Ben Hassine, and *Digital safety in context: Perspectives on digital security training and human rights realities in the Arab world*,[9] by Reem al-Masri, both of which cited the dataset as a source. The ADRD was also presented as example of data journalism and research on the blog of the Research Center at the CUNY Graduate School of Journalism.[10]

[2] https://www.igmena.org

[3] http://smex.silk.co

[4] As of August 2016, the Silk platform has been deprecated, meaning that despite allowing new accounts to be created, no technical support or development resources are being provided to the platform.

[5] The Silk platform is being taken offline on 15 December 2017. SMEX is currently working with the human rights information management NGO HURIDOCS (https://www.huridocs.org) to develop a new platform to host the data.

[6] Inductive research is a bottom-up approach by which a researcher begins with observations to detect patterns that can form the basis for a hypothesis that can be tested and developed into theory. It contrasts with deductive research that aims to test a hypothesis to prove a theory.

[7] Ben Hassine, W. (2016a). *The Crime of Speech: How Arab Governments Use the Law to Silence Expression Online*. Electronic Frontier Foundation. https://www.eff.org/pages/crime-speech-how-arab-governments-use-law-silence-expression-online

[8] Ben Hassine, W. (2016b). *Digital rights advocacy in the Arab world and the Universal Periodic Review*. Association for Progressive Communications. https://www.apc.org/en/pubs/digital-rights-advocacy-arab-world-and-universal-p

[9] Al-Masri, R. (2016). *Digital safety in context: Perspectives on digital security training and human rights realities in the Arab world*. Association for Progressive Communications. https://www.apc.org/en/pubs/digital-safety-context-perspectives-digital-securi

[10] http://researchcenter.journalism.cuny.edu/tag/tool /

Being able to release this data on Silk in a publicly usable format established proof of concept for the datasets and their utility. Equally important, it helped SMEX secure funding to further refine the data collection methodology and expand the scope of its application from the Arab region to similar initiatives worldwide, as APC-IMPACT has done with its research on the criminalisation of online speech in six countries in South Asia and Southeast Asia. Furthermore, it helped lay the groundwork for the transformation of the methodology into a shared technical standard whose adoption would not only facilitate free and open access to digital rights law and case law in countries worldwide, but also enable the combination of legal source data with other datasets, comparative analysis between jurisdictions, and the charting of global trends in digital rights.

The SMEX methodology was adapted for use in this report, *Unshackling Expression*.

Grounded, global and adaptable

Between August 2016 and July 2017, SMEX, working with legal adviser Nani Jansen and technology adviser Seamus Tuohy and a cohort of legal researchers, designed, tested and transformed a methodology to map, organise and make available digital rights-related laws. The result is the third version of the ADRD,[11] which now includes more than 240 laws and, where possible, their translations; relevant articles of law; bills; and case law.

In this phase of the project, the aim was not only to expand the ADRD but also to build on earlier, crowdsourced phases of development to produce criteria and a process for collection of law and case law that were 1) rigorous enough to gain credibility among human rights researchers and legal professionals, and 2) flexible enough to be adapted by civil society actors around the world, and particularly in the global South, for multiple purposes across multiple channels.

To achieve this, SMEX mapped out a multi-step process that began with soliciting feedback from about a dozen current and potential users of the dataset to better understand their wants and needs. Then, we aimed to ground the methodology in current digital rights definitions and legal practice, reviewing influential literature and initiatives, including rights charters and analysis; UN resolutions and reports by special rapporteurs; and analogous law aggregation projects such as the Centre for Law and Democracy's Global RTI Rating[12] and Graham Greenleaf's Global Tables of Data Privacy Laws and Bills.[13] Meanwhile, our discovery of the decades-old Free Access to Law Movement[14] and the many online legal information institutes (LIIs) it has spurred around the world helped anchor our project to a broader context in which "ready access to law is a human right."[15] Next, we triangulated several approaches to setting criteria for the inclusion of specific laws and related documents – this time including articles, bills and case law – in the dataset, as well as establishing a five-category framework that would help both expert and non-expert researchers locate them.

Once we had a strong rationale for the inclusion of legislation and/or case law in the dataset, we recruited and trained a team of a dozen legal researchers to identify relevant legislation from the 22 countries of the Arab League and code the results in a country-specific research workbook. This information will eventually be transformed into a web- and API-accessible database that anyone can access.

Below we explain how the underpinnings of the refined methodology evolved with each step. We also detail the implementation of the methodology, including logistical stumbling blocks that we hope other adopters will avoid, and note recommendations for improvement. Finally, we share our plans for further development and solicit feedback. The Resources section at the end of this chapter makes available the current methodology and research guidance.

Developing the methodology: Step by step

Step 1: Taking stock: Stakeholder interviews inform the methodology

In October 2016, we conducted more than a dozen interviews with users of the Silk-hosted dataset. Users came both from within the Arab region and beyond and included human rights lawyers, researchers at advocacy organisations, experts in business and human rights, technologists, journalists, as well as a policy director and legal counsel at a global social media platform. During these interviews, we asked stakeholders what they currently

[11] It is not yet public, pending expert review of the data.

[12] www.rti-rating.org

[13] Greenleaf, G. (2015). Global Tables of Data Privacy Laws and Bills (4th edition, January 2015). https://ssrn.com/abstract=2603502

[14] www.fatlm.org

[15] Jamar, S. D. (2001). The Human Right of Access to Legal Information: Using Technology to Advance Transparency and the Rule of Law. *Global Jurist Topics, 1*(2), 1-14. https://ssrn.com/abstract=1148802

used the dataset for and what more they would like to be able to do with it, such as which legal processes the dataset could support and whether there were other datasets that, if combined with the legislation data, would yield deeper insights. From these interviews, we develop a list of recommendations for improving the datasets that included:

- Establishing a working definition of digital rights as a foundational framework to develop criteria for which laws, cases and decisions are included.
- Including context on the legal landscape that encompasses the type of legal system, relevant portions of major pieces of legislation, specific case law, and relevant international legal instruments binding on the state.
- Including draft laws, because it is easier to challenge a bill than to reform legislation.
- Including specific provisions of laws, such as sections or articles governing digital rights.
- Including the most important of well-known court decisions to understand how the judiciary perceives the issues.
- Including corporate policies, terms of service, privacy policies, etc.
- Indicating the source of the law or translation, and whether it is official, as well as creating a source-ranking methodology for secondary sources (i.e., ranking of some reports would be higher than others) and categorising sources as either primary or secondary.
- Refining the categorisation of the laws and adding subcategories and tags to make data more granular and searchable and in line with existing taxonomies and schema.
- Noting discrepancies between international treaties and national constitutions and laws.
- Considering the addition of laws that impact association and assembly, social media companies and applications, such as VoIP restrictions or shutdown decrees.

Interviewees also shared ideas about specific functionalities for the dataset, as well as its design, maintenance and expansion. Even ethical considerations arose, as some warned that highlighting court cases without redacting names could potentially re-victimise people.

After consulting with the legal and technical advisers, it was clear that we would not be able to include all items on the wish list. We prioritised those elements that we considered essential to building a minimum viable data product, based in part on the frequency with which they were mentioned. These included being more explicit about how we define digital rights to limit the scope of the inquiry; sourcing the documents and translations so that their provenance and whether they were official or unofficial was easily verifiable; identifying relevant provisions within documents to help users pinpoint those articles that are most directly connected to digital rights; and including draft laws, where possible.

Step 2: Developing a working definition of "digital rights"

Creating a database of legislation related to digital rights is a simple notion in theory; in practice, it is quite something else. To quote privacy scholar Graham Greenleaf, who has catalogued the world's data privacy laws, "Before answering a simple question" – like, how many countries have data privacy laws? – "it is sometimes necessary to answer some more complex questions first."[16]

For the purposes of his research, Greenleaf needed to define "What is a country?", "What is a law?", "What scope must a law have?", "What data privacy principles must a law include?" and "How effective must a law be?" By considering and answering these questions, Greenleaf established "the minimum criteria that reasonable and impartial observers could agree constitute a 'data privacy law' or 'data protection law' when satisfied."[17] Because the datasets intend to catalogue legislation affecting digital rights we also need to ask, What are digital rights? and, How will we identify and locate a law or other legal instrument that affects digital rights?

Defining "digital rights"

Perhaps surprisingly, there is no commonly accepted definition of digital rights. Nor is it clear when the term first emerged.[18] The European Digital

[16] Greenleaf, G. (2014). Sheherezade and the 101 data privacy laws: Origins, significance and global trajectories. *Journal of Law, Information & Science, Special Edition: Privacy in the Social Networking World, 23*(1). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2280877

[17] Ibid.

[18] We theorise that it could have emerged as a derivative or truncation of the phrase "digital rights management" or DRM, a process by which code embedded into multimedia files, like movies or songs, prevents users from sharing files. Searching the archive with the term "digital rights" brought up 98 pages of results from as early as 2003. Until the late 2000s, most of the results containing "digital rights" pertained to DRM, a key advocacy issue for the Electronic Frontier Foundation.

Rights initiative (EDRi), a Brussels-headquartered "association of civil and human rights organisations from across Europe,"[19] was founded in 2002, perhaps reflecting one of the earliest uses of the term. People have, however, been drafting bills of internet rights since at least the mid-1990s,[20] and over the last decade a strong body of interdisciplinary literature has emerged that considers digital rights as an extension of human rights with specific characteristics and implications.[21] The UN Human Rights Council, for instance, has affirmed multiple times:

> [T]he same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with article 19 of the Universal Declaration of Human Rights and of the International Covenant on Civil and Political Rights.[22]

Notwithstanding these efforts and milestones, digital rights has not yet emerged as a field of its own. Referring to the literature that does exist, internet scholars Rikke Jørgensen and Meryem Marzouki write:

> The majority of these sources, however, are not anchored in a theoretical framework but present empirically grounded studies of 1) opportunities and threats to established human rights standards by use of communication technology, in particular the right to privacy and the right to freedom of expression, or 2) cases that focus on the use of technology for human rights and social change, or 3) standard-setting that seeks to establish norms for human rights protection in the online domain. At present there is a lack of scholarship connecting the human rights challenges raised by these numerous studies with their theoretical context.[23]

In addition, most of the many organisations[24] that advocate and promote digital rights similarly reflect this practical grounding by referring to other established normative frameworks, such as civil liberties and human rights, and then situating them semantically "online" or "on the internet". Thus, the phrase "digital rights" does not yet refer to a specific set of rights or theory of rights. Rather, it is shorthand for a broad group of rights issues raised when interpreting human rights and civil liberties in digitally networked spaces.[25]

Given, as Jørgensen and Marzouki note, that "the modalities of the online realm provide significant challenges to human rights protection, many of which remain largely unexplored" – such as the so-called right to be forgotten or the right to access the internet[26] – what exactly is a digital right is still left open to interpretation, posing potentially significant challenges, one of which for our purposes is whether the term can be used as the cornerstone of a rigorous and replicable research methodology. One outcome of this conceptual instability is a propensity of digital rights actors to "pick up" their "right of interest, with limited attention to the overall framework and the interdependence between the full architecture of rights."[27] In short, the question that emerges for our methodology is, Which rights satisfy the definition of digital rights when looking at the legal framework and which do not?

[19] https://edri.org/about

[20] Gill, L., Redeker, D., & Gasser, U. (2015). *Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights*. Berkman Center Research Publication No. 2015-15. https://ssrn.com/abstract=2687120

[21] Jørgensen, R. F. (2016). *Negotiating boundaries: How platforms shape human rights*. ipp.oii.ox.ac.uk/sites/ipp/files/documents/boundary%2520OII.pdf

[22] Human Rights Council. (2016). The promotion, protection and enjoyment of human rights on the Internet. A/HRC/RES/26/13. https://digitallibrary.un.org/record/845727/files/A_HRC_RES_32_13-EN.pdf

[23] Jørgensen, R. F., & Marzouki, M. (2015). Reshaping the Human Rights Legacy in the Online Environment. *L' Observateur des Nations Unies, 38*, 17-33.

[24] For instance, on its home page, Access Now, an international non-profit advocacy organisation founded in 2009, says it "defends and extends the digital rights of users at risk around the world." Nowhere on the site, however, does it define digital rights. It is left to visitors to interpret what digital rights are via the programme areas it covers: business and human rights, digital security, freedom of expression, net discrimination, and privacy. The San Francisco-based Electronic Frontier Foundation (EFF), founded in 1990, regularly uses the term "digital rights" in advocacy and press communications. Its mission, however, is phrased as "defending civil liberties in the digital world," including user privacy, free expression, and innovation. The organisation also maintains a web page called "Themes in Digital Rights", but does not define digital rights, except as through the themes listed, which include NSA spying, fair use, transparency, freedom of speech, drones, and blogger's rights, among others. Other digital rights advocacy organisations similarly skirt defining the term, except through their work. EDRi, for example, defends "rights and freedoms in the digital environment," in programme areas such as privacy, copyright, self-regulation, freedom of expression, security and surveillance. The objective of the Chile-based Derechos Digitales, whose name means "digital rights" in Spanish, is "the development, defence and promotion of human rights in the digital environment," encompassing free expression, privacy and personal data, and the rights of authors and access to knowledge. Digital Rights Ireland, meanwhile, "is dedicated to defending Civil, Human and Legal rights in a digital age." It currently campaigns on the issues of privacy and data retention, web blocking and filtering, and copyright reform.

[25] Here, we adopt sociologist Zeynep Tufecki's definition of "networked" from the preface to her 2017 book *Twitter and Teargas: The Power and Fragility of Networked Protest*, as "the reconfiguration of publics and movements through assimilation of digital technologies into their fabric."

[26] Jørgensen, R. F., & Marzouki, M. (2015). Op. cit.

[27] Ibid.

In the absence of an agreed-upon definition of digital rights, we had two choices: 1) to find another term to describe the scope of the datasets we wanted to build or 2) to propose a working definition of digital rights that met our primary goal of being able to set clear criteria for the inclusion of legal instruments in our database. In the first case, we considered other terms, such as "internet rights",[28] which had been used early on by organisations like APC, or "internet freedom", a phrase that originated with the administration of former US Secretary of State Hillary Clinton. "Internet freedom",[29] we decided, was too closely tied to US government policy. Meanwhile, because it describes a configuration of technology, "internet" itself also seemed unnecessarily restrictive, or at least more restrictive than a broader term such as "digital", which could more easily encompass emerging technologies and locations other than the internet (such as data storage, biometrics and drones). We were also aware of other initiatives, like the Africa ICT Policy Database,[30] which aimed to collect all laws affecting information and communications technologies (ICTs). But for our purposes of identifying laws that had a direct impact, positive or negative, on human rights in digitally networked spaces, broadening the scope to include all laws that impact ICTs was deemed too broad.

Without a satisfactory alternative and given the already prevalent use of "digital rights" in the mission statements and names of so many of our peer organisations around the world, including in translation, we opted to propose a working definition based on existing literature and usage. We began by reviewing many of the key charters of digital rights and in a stroke of luck (searching the open Social Science Research Network) discovered that a 2015 article titled "Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights", by Lex Gill, Dennis Redeker and Urs Grasser, had already done much of our work for us.

Developing a working definition of "digital rights"

"Towards Digital Constitutionalism?" reviews 30 charters of internet or digital rights cumulatively endorsed by hundreds of groups from multiple sectors. The earliest charter is dated 1999; the most recent is from 2015. They include laws (adopted and proposed), official positions, and advocacy statements. From these charters, the authors extracted 42 aspects of digital rights in seven categories: basic or fundamental rights and freedoms, general limits on state power, internet governance and civic participation, privacy rights and surveillance, access and education, openness and stability of networks, and economic rights and responsibilities.

The authors observed that the charters all depend on the language of the Universal Declaration of Human Rights and to varying extents that of the ICCPR and the International Covenants on Economic, Social and Cultural Rights (ICESCR). The charters also all exhibit a "constitutional character", speak to a political community, aspire toward formal recognition and legitimacy within that community, and share a degree of comprehensiveness.[31]

Meanwhile, the bills are far from universal. They differ in their content and focus, their prioritisation of rights, the stakeholders involved and political communities targeted, contexts of reference, and drafting and review methods. Despite their common spirit, their diversity presents a challenge when trying to 1) decide what is a digital right, and 2) assess whether that right has been encoded in law, further underscoring the observation that there is no universal understanding or agreement on which rights constitute digital rights or how they are interconnected.

For example, advocates within the digital rights sector disagree on whether there is a right to access the internet or a right to be able to delist oneself from search results and be "forgotten". Both these "rights" appear in the list. The charters also acknowledge that other rights – workers' rights, children's rights, sexual rights – are significantly affected by digital technologies and in digital spaces. UNESCO considers the right to cultural diversity in education a kind of digital right in its book on internet governance, but does not mention the rights to association and assembly, as APC does in its conception of digital rights.[32]

Meanwhile, internet rights are being defined as they are viewed through the lenses of rights and legal frameworks at the international, regional and national/local levels – both in legally binding treaties and legislation and in case law – as well as through the policies and practices of private-sector corporations, adding further complexity to understanding what is a digital rights law or a law that

[28] Released in November 2006, the Association for Progressive Communications' Internet Rights Charter was one of the earlier charters of digital rights. https://www.apc.org/en/pubs/about-apc/apc-internet-rights-charter

[29] See, for example: https://www.state.gov/j/drl/internetfreedom/index.htm

[30] www.ictpolicy.org

[31] Gill, L., Redeker, D., & Gasser, U. (2015). Op. cit.

[32] "Internet rights are human rights" multimedia toolkit, Association for Progressive Communications. www.itrainonline.org/itrainonline/mmtk/irhr.shtml#Intro

implicates digital rights, especially when interpreting those rights in local jurisdictions. In addition, the ad hoc nature of establishing and interpreting digital rights through the law also means that our understanding of legal frameworks for digital rights at any level is far from comprehensive.

With all this in mind, we drafted a working definition of digital rights that attempts to capture their interdisciplinary, multidimensional, evolving nature. We wanted to highlight that these rights cannot be traced to a single authority or source, but rather are a product of distributed work, like the charters themselves. Further, we wanted to recognise that the spaces in which digital rights exist, like human rights, are unbounded. Thus, we adopted the phrase "digitally networked" to encompass not just the browsable internet but other digital networks. This is becoming even more important with the growing recognition that even people who are not connected online are increasingly affected by what happens in the digital sphere.[33] Finally, we wanted to acknowledge that rights can be situated not just in content and interaction but also in other protocols, such as algorithms, on these networks or at their nodes, which come in the form of objects (devices) and in the form of expressions of our identities, whether individuals or groups, hidden, imagined, or in plain sight. Below is the definition we drafted. As a cornerstone of the refined methodology, it was meant to establish a reference point by which one can judge whether a law affects digital rights. It is a work in progress.

Working definition: "Digital rights" describe human rights – established by the Universal Declaration of Human Rights, UN resolutions, international conventions, regional charters, domestic law, and human rights case law – as they are invoked in digitally networked spaces. Those spaces may be physically constructed, as in the creation of infrastructure, protocols and devices. Or they may be virtually constructed, as in the creation of online identities and communities and other forms of expression, as well as the agency exercised over that expression, for example, management of personally identifiable data, pseudonymity, anonymity and encryption. Such spaces include but are not necessarily limited to the internet and mobile networks and related devices and practices.

Our working definition of digital rights served as a touchstone as we developed the rest of the methodology. In particular, it helped us devise a strategy for locating relevant legislation and then categorising that law.

Step 3: Establishing criteria and a research path to identify relevant legislation

Just as digital technologies have been integrated into every aspect of life, we can expect them to appear in multiple and increasingly diverse areas of law, from constitutions that make internet access a right, to health care laws that aim to protect patients' data privacy, to anti-terrorism laws that restrict speech glorifying violent extremism on online platforms. Radar Legislativo,[34] a legal data initiative from Brazil that tracks draft laws, recently counted 303 bills that affect the internet under review by that country's National Congress.[35] So even with the working definition in hand, we still needed to set criteria to help researchers narrow the field of inquiry and also give them a reasonable degree of certainty that the laws they found were in fact the laws they were looking for. To do this, we employed two complementary strategies: first, we looked at how Greenleaf identified data privacy laws, and second, we tried to locate the most likely areas in a legal framework where a researcher would find laws related to digital rights.

In Greenleaf's model, a researcher could identify a data privacy law in one of three complementary ways. First, they could look for laws that address data privacy principles, as defined by a "'strong consensus' that has emerged as to what are a set of twelve 'fair information principles'."[36] Even a law with provisions that address only some of the principles could qualify the law as a data privacy law. To apply this to the problem of identifying a digital rights law would mean identifying the kinds of laws that routinely affect digital rights, or that are designed explicitly to establish norms for digitally networked spaces. While we know of no "strong consensus" about what laws might comprise a list of digital rights-related laws, we can deduce from the laws we and others have collected that it would likely include data privacy laws, right to information laws, etransactions laws, anti-cybercrime laws, and broad internet laws like Brazil's *Marco Civil da Internet* (Civil Rights Framework for the Internet).[37]

[33] Tufecki writes "'digitally networked movements' or 'networked movements,' does not mean 'online-only' or even 'online-primarily.' Rather, it's a recognition that the whole public sphere, as well as the whole way movements operate, has been reconfigured by digital technologies, and that this reconfiguration holds true whether one is analyzing an online, offline, or combined instantiation of the public sphere or social movement action."

[34] https://www.radarlegislativo.org

[35] Conversation with Kimberly Anastácio, Coding Rights, 18 October 2017.

[36] Greenleaf, G. (2014). Op. cit.

[37] www.cgi.br/pagina/marco-civil-law-of-the-internet-in-brazil/180

Conversely, a researcher might define a law as affecting digital rights even if its scope was not limited to the internet and digitally networked spaces. For instance, an intellectual property law may deal with works produced in both analogue and digital media, but its sections or provisions dealing specifically with the internet or digitisation would qualify it as a law affecting digital rights. With that in mind, we could use Gill et al.'s 42 rights[38] as a kind of checklist when analysing laws of any kind for their effects on digital rights.

Finally, because law is constituted not just by static text but by interpretation, Greenleaf emphasises the importance of international law and soft law. In the case of data privacy laws, he specifically refers to the OECD Privacy Guidelines of 1981 and the Council of Europe Data Protection Convention 108 of 1981. From this approach, we can assess whether a law affects digital rights, or a specific digital right, based on the growing body of analysis of digital rights within international covenants and related human rights frameworks, such as the ICCPR and ICESCR, special rapporteur reports, and their derivatives, including the digital rights charters, data privacy and access to information frameworks mentioned above, as well as other frameworks such as the UN Guiding Principles on Business and Human Rights, etc. We would add to that interpretation of law by courts and tribunals in case law and other types of precedent that would afford insight not only into how laws were being applied but also into how laws with no overt relationship to digitally networked spaces might be adapted or abused.

We believed this triangulated approach would help researchers recognise a digital rights law when they saw it. Still, we knew that researchers could not and would not read every law on the books to decide whether or not they affected digital rights. With this in mind, we aimed to ease the search further by offering several entry points for their inquiries. Working from types of law developed for the existing laws in the dataset and category structures devised by Gill et al.[39] and ARTICLE 19,[40] we developed five categories[41] into which we believed the majority of laws would fall: 1) legal foundations, 2) fundamental rights and freedoms, 3) governance of online and networked spaces, 4) sectoral laws, and 5) other laws.

In the *legal foundations* category, we intended to collect laws that (1) form part of the foundation of the legal system and address universal rights, responsibilities, due process or, following Gill et al., other "general limits on state power,"[42] and (2) contain provisions that refer or apply to how an individual can exercise their rights and freedoms in digitally networked spaces. Examples of laws that would fit in this category include constitutions, basic laws, penal codes and codes of procedure.

We described laws pertaining to *fundamental rights and freedoms* as those laws and regulations that (1) establish norms for, enable or restrict the exercise of fundamental rights and freedoms – including the right to freedom of expression, privacy, freedom of religion and freedom of association – and (2) contain provisions that refer or apply to how an individual can exercise these rights and freedoms in digitally networked spaces. Examples are press laws or laws protecting or limiting the right to privacy, freedom of expression or to access information.

The drive to establish new norms in the digitally networked sphere and to mitigate the negative potential of digital technologies – realised as computer fraud and identity theft, the circulation of child pornography, online harassment, so-called "revenge porn" and doxxing, for instance – has been the genesis of many newer laws and regulations explicitly for *governing online, networked spaces*, a category developed to collect laws such as data privacy and protection laws, anti-cybercrime laws, and net neutrality regulations. Here, we might also find laws or judicial decisions that acknowledge the new so-called right to be forgotten, a concept that did not exist before the internet.

Digital technologies have had a pervasive effect on some industries and sectors, and the laws and regulations in these sectors are sometimes some of the first that deal with the new modalities of the online realm directly and in depth. To acknowledge this, we created a category for *sectoral laws*. Specifically, we sought laws and regulations that (1) update or establish norms that implicate digital rights in a specific sector, such as banking or health care, or for a specific group of people, such as government employees, and (2) contain provisions that

[38] Gill, L., Redeker, D., & Gasser, U. (2015). Op. cit.

[39] Gill, Redeker and Gasser organised the 42 rights extracted from the 30 charters into seven categories: Basic or Fundamental Rights and Freedoms, General Limits on State Power, Internet Governance and Civic Participation, Privacy Rights and Surveillance, Access and Education, Openness and Stability of Networks, and Economic Rights and Responsibilities.

[40] ARTICLE 19 used six categories of inquiry when analysing how the laws in the Internet Legislation Atlas (affected digital rights in seven Middle Eastern countries: constitutional protection, regulation of online content, regulation of media workers, regulation of internet intermediaries, surveillance and data protection, and access to the internet and net neutrality. See: https://internetlegislationatlas.org/#/about/executive-summary#breakdown

[41] ADRD Research Guidance Document (see the Appendix to this chapter).

[42] Gill, L., Redeker, D., & Gasser, U. (2015). Op. cit.

refer or apply to how an individual can exercise their rights and freedoms in digitally networked spaces. Examples here are laws on electronic patient files, consumer protection, or issues such as privacy in the workplace.

Finally, in some countries, laws having no specific language on digital rights had been used to repress free expression. For example, in Tunisia, drug laws have been used to prosecute alleged speech crimes.[43] Around the world, anti-terror laws are regularly being used against journalists.[44] In the US, a law meant to curtail copyright infringement was ultimately rejected for its potential to chill speech.[45] And in Vietnam, tax laws are regularly used to prosecute bloggers.[46] To acknowledge this phenomenon, we created a category of *other laws* to capture the counterintuitive and sometimes systematic use of laws not in the first four categories. Identification of these laws often depends on monitoring and analysis of case law.

Because legal systems are always changing, being amended, reinterpreted, appealed, the triangulation process and the five-category structure did not always support clear-cut decisions. The research process surfaced differing opinions about which laws qualified as affecting digital rights, where to categorise a law, or whether one law could fit into two categories. For example, some researchers elected not to include press and publications laws if they did not expressly mention electronic media. Others saw the potential for these laws to be used to restrict digital spaces, so they listed them. Then, there were divergent approaches to categorisation: does a press and publications law belong in the fundamental rights and freedoms category or is it a sectoral law?

While perfect precision is not possible, the aim was to help researchers blaze a path through complex and evolving legal systems by offering several entry points where one might find digital rights-relevant law. Grounding the research and review process in a consistent approach would yield more or less comparable results that could be further refined during peer and expert reviews. The next challenge was to transform these underpinnings – the working definition of digital rights, the triangulated criteria for identifying relevant laws, and the five-category structure – into a usable, adaptable research methodology and to launch the research process.

Step 4: Concretising and implementing the methodology

We had three main goals when developing the research methodology and guidance. First, we wanted it to be simple and accessible enough that any researcher – even ones without legal research experience – could use it. Second, we wanted it to be flexible enough that it could be adapted by other initiatives around the world doing similar types of work. Third, we wanted to be able to share this methodology and a collection of user scenarios for using the data with a technologist to develop a machine-readable data model that would undergird future applications that make use of the data.

The implementation phase by and large demonstrated that the methodology successfully met our goals of being rigorous enough to gain credibility among users seeking verified legal information yet flexible enough to be adapted to different jurisdictions and legal themes. There were challenges, however, and for future applications, we have identified opportunities for further refinement in each section below.

Creating data collection tools and guidance

For data collection, we created a multi-tab workbook in Google spreadsheets and individual folders for each country on Google Drive. We then produced two research guidance documents: ADRD Research Guidance and ADRD File Management and File-Naming Formats. Both these documents are included in the Resources section.

The data collection workbooks functioned as an index for three key types of information: original laws, case law and draft law. Researchers were asked to name the laws in the original language and to upload the document to a corresponding Google Drive folder – using the prescribed file-naming convention – and indicate the link to the law in that folder. For each type of information, we also asked for relevant translations. For laws and bills, we asked researchers to identify the key provisions that affect digital rights. For case law, we asked for a summary of the impact of the decision on digital rights. In addition to this key data, we also gathered metadata such as dates, keywords and sources. The workbooks also included a cover sheet with links to the research guidance, a tab where researchers

[43] Ben Hassine, W. (2016a). Op. cit.

[44] Ginsberg, J. (2017, 26 October). Targeting journalists in the name of national security. *Index on Censorship*. www.indexoncensorship.org/2017/10/targeting-journalists-name-national-security

[45] SOPA/PIPA: Internet Blacklist Legislation, Electronic Frontier Foundation. https://www.eff.org/issues/coica-internet-censorship-and-copyright-bill

[46] Jansen, N. (2013, 9 July). Advocates Keep Spotlight on Le Quoc Quan. *Global Voices*. https://advox.globalvoices.org/2013/07/10/advocates-keep-spotlight-on-le-quoc-quan

could note laws currently in the dataset that should be removed, a sheet asking researchers to note their general sources of information, and a locked data validation tab. The workbooks summarised relevant research guidance at the top of each column.

The country folders contained five subfolders and two spreadsheet documents. Two folders corresponded to the laws and draft laws, each of which had subfolders for each category of law. A third folder was for case law, a fourth for translations, and the fifth was for secondary sources. One spreadsheet listed the laws currently in the ADRD dataset and the second was the new data collection workbook.

For further refinement: While Google Drive and Docs satisfied our needs for an easily accessible and configurable tool – especially for being able to share documents among several users and track comments between them – there was at least one researcher who had trouble negotiating the folder structure and creating links to shared files. In addition, we used available data verification features to populate dropdown menus from one spreadsheet to another. This worked seamlessly when connecting original laws to their translations, for example, but not as well when connecting articles of law to primary or secondary legislation. For example, on the key provisions worksheet, researchers were asked to enter relevant articles. These entries populated a dropdown menu in the case law spreadsheet. But when a researcher wanted to indicate which article was relevant to the case law, they would sometimes see two articles with the same number but from different laws and not know which to choose, potentially leading to documentation errors. In future iterations of the workbook, we will explore tools that would make it more difficult for researchers to make these and other kinds of coding errors. Finally, organisations that prefer not to use Google products for security reasons may also want to adapt the workbook to other tools.

Recruiting and orienting researchers

Earlier data collection was conducted by volunteers and journalists, but not legal experts. Because the refined methodology relied much more on an understanding of law and legal systems, we prioritised working with lawyers preferably with expertise in the countries they were researching, or at least in the region. We launched a 10-day call for legal researchers[47] and although our timeline was short we received 16 applications, among them researchers who had worked on the previous versions. Twelve candidates were contracted to do one round of research and one round of peer review. Some candidates took on more than one country. Researchers came from Egypt, Jordan, Lebanon, Morocco, Oman, Palestine, Sudan, Syria, Tunisia and Yemen, as well as the US and France.

Researchers were asked to attend one of two one-hour virtual orientation sessions[48] held by SMEX and led by legal adviser Jansen. Before the orientation session, researchers were able to review the data collection workbook and the research guidance and make suggestions for refinements. The sessions began with an overview of the scope of work and then relied on researchers to ask questions to clarify any unclear guidance. They also noted specificities within national legal systems that would pose challenges to capturing data in the format we had provided. For example, it was noted that in some jurisdictions, amendments are issued separately from the laws to which they apply, rather than integrated into a reissued law. This, plus questions about whether regulations should also be included, resulted in adding a column that qualified laws as either primary or secondary. Researchers raised concerns about different definitions of case law, which was clarified as referring to “judicial decisions and other jurisprudence that constitutes an authoritative interpretation of the law.”[49] Also with regard to case law, some researchers relayed that in their jurisdictions the names of the parties are not used to name the cases. To create unique case names, researchers were asked to assign unofficial names to the cases. These notes and others were captured in an addendum to the research guidance document (available in the Resources section at the end of this article) called ADRD Workbook Updates Doc.[50]

After the sessions, a Google Group mailing list was set up where researchers could ask questions during the data collection process and further refine the research guidance as needed.[51] More active researchers posed sporadic queries to the mailing list, but many remained quiet, making it necessary to follow up on an individual basis, which was burdensome given that one person was managing 12 researchers and 22 workbooks.

[47] SMEX Seeks Legal Researchers for Arab Digital Rights Database. https://docs.google.com/document/d/1SGW9STW-tx5Y34LmfHoSJhOmnlobfQcsuGNmLIGvamo/edit

[48] Budget constraints prevented us from being able to host an in-person training workshop.

[49] https://docs.google.com/document/d/11NAys-JDDiU4Ht4VLyV4HPH3dzVqBxKwrsvUYTIoLQE/edit

[50] Ibid.

[51] ADRD Summary Report, August 2017, submitted by Nani Jansen.

For further refinement: In retrospect, the short time frame for recruiting and training researchers led to some inconsistencies in the research results. In particular, the legal adviser's review revealed that not all researchers demonstrated the same understanding of the level of detail being requested, which has led SMEX to conduct additional rounds of review. In future, we recommend that, when resources are available, in-person trainings on the research methodology and workbook should be organised and attendance should be a condition of payment. A longer, multi-round recruitment process, with some kind of assessment to measure the researcher's capacity and eye for detail, would also be useful and help expedite data review and verification.

Data collection and review: Findings and challenges

After five months' preparation, data collection began in early March 2017. Researchers were given one month to complete the original research process and one month to complete their peer review, which involved checking the folder and workbook of a second country.

Three researchers dropped out before the research was complete for health and family reasons. Meanwhile, one researcher revealed late in the process that they did not read Arabic. Also, because some researchers were behind schedule, the peer review process was also delayed. Ultimately, the first round of original research and peer review concluded in June 2017.

In July 2017, SMEX and the legal adviser conducted an overall review of all the workbooks. In all, the law catalogues grew from 142 in the first dataset to around 240, the vast majority of them with official or unofficial translations. Dozens of key provisions were identified. Several draft laws were noted, and case law, a completely new type of information in this version of the ADRD, was identified in six countries.[52] Following a final review by SMEX and in-country experts, the expanded datasets will be made public.

For further refinement: As mentioned above, SMEX has added two more rounds of review to ensure that the data we have is as accurate and up-to-date as possible. Unfortunately, this has delayed making the data available, which could also compromise its accuracy, if too much time passes. To avoid such delays in the future, we recommend that research supervisors implement a phased approach with interim milestones. For example, data could be collected, reviewed and verified for one worksheet at a time and combined with periodic group calls to raise and resolve concerns or challenges encountered. This would not only help ensure that researchers develop a shared understanding of the nuances of the research process but will also yield better results that can be publicised more quickly.

Finally, while we included draft laws and provisions and case law in the current workbook in response to stakeholder requests for this data, we are delaying their integration into the public dataset pending more detailed research and review. Gathering data about case law posed several problems with regard to not only locating and sourcing decisions but also in developing a consistent approach to explaining how cases interpret the relevant laws, which is essential to being able to publish authoritatively on their impact. In subsequent phases of the project, we will explore addressing such challenges by integrating into the methodology existing approaches to analysing case law, such as that of Columbia University's Global Free Expression Case Database.[53]

The future roadmap

Perhaps unlike other research methodologies, the one for the Arab Digital Rights Datasets was also designed to be expressed as a data model, or a conceptual framework to organise and standardise the data collected. Rendering the methodology as a data model makes it much easier to share, extend, combine and repurpose information, especially by machines. In parallel with the data collection and review process, we worked with technologist Seamus Tuohy to create the data model for the ADRD and a related API, or application programming interface. An API is a piece of code that sits between a database and a graphic user interface (GUI) that calls information from the database according to what a user needs.

This data model and API will be used to build a database of the Arab laws collected and make the data both human and machine-readable. But it is our hope that these technical interpretations of the methodology will also afford other organisations conducting similar research the opportunity to make their data more available and accessible too. To this end, SMEX is now forming a working group to explore the potential for this data model to become a global standard for aggregating, organising

[52] Case law was identified in only six countries: Egypt, Jordan, Kuwait, Lebanon, Morocco and Mauritania.

[53] https://globalfreedomofexpression.columbia.edu/cases

and analysing the evolution of digital rights law and to encourage other researcher-technologist teams to develop new applications that draw on this data and/or combine it with other datasets. Other challenges we will turn our attention to as the project develops include devising strategies for keeping the information up-to-date across many countries, as well as for tracking draft laws and new cases. If you would like to be a part of this group, we encourage you to let us know at adrd@smex.org.

Resources for implementing the methodology

ADRD Research Guidance
https://docs.google.com/document/d/1vxKMC-GIXcQoFPqubRyJS9Io8Jq9hBboEE5a7IcvoxCs/edit#

ADRD Workbook Updates Doc
https://docs.google.com/document/d/11NAys-JD-DiU4Ht4VLyV4HPH3dzVqBxKwrsvUYTIoLQE/edit

ADRD File Management & File-Naming Formats
https://docs.google.com/document/d/17ALaT-otCXy-8evSWscoKcF5VFmVdUM-xP_MWAPUH37M/edit

ADRD Sample Data Collection Workbook: Egypt
https://docs.google.com/a/smex.org/spreadsheets/d/1rQoRdXDBqLWgyC-gWEmOUzAkdClLt7U2YRTHFSh1JbFo/edit?usp=sharing

Data Model and API
To access the current versions of the data model or API, please email jessica@smex.org.

GLOBAL INFORMATION SOCIETY WATCH 2017 SPECIAL EDITION

UNSHACKLING EXPRESSION:
A study on laws criminalising expression online in Asia

Freedom of expression and opinion online is increasingly criminalised with the aid of penal and internet-specific legislation. With this report, we hope to bring to light the problematic trends in the use of laws against freedom of expression in online spaces in Asia.

In this special edition of GISWatch, APC brings together analysis on the criminalisation of online expression from six Asian states: Cambodia, India, Malaysia, Myanmar, Pakistan and Thailand.

The report also includes an overview of the methodology adapted for the purposes of the country research, as well as an identification of the international standards on online freedom of expression and the regional trends to be found across the six states that are part of the study. This is followed by the country reports, which expound on the state of online freedom of expression in their respective states.

With this report, we hope to expand this research to other states in Asia and to make available a resource that civil society, internet policy experts and lawyers can use to understand the legal framework domestically and to reference other jurisdictions.

GISWatch 2017
SPECIAL EDITION
https://www.GISWatch.org

SUPPORTED BY

EUROPEAN UNION

INTERNET POLICY OBSERVATORY