Report

Research on digital security within Grassroot organizations in chiapas

Luchiendo
Comunicación
Cultura Digital

Report

Research on digital security within Grassroot organizations in Chiapas

SPECIAL THANKS:
To the organizations that participated on this research, to Access Now for the support to carry out this project, and to all the people who have contributed for the development of this report.

CREDITS:
Coordination: Sursiendo
Texts and edition: la_jes and dom
Review: Paola Ricaurte
Editorial Design: Irene Soria
English translation: Nàdege.
Images: la_jes

Index

0. Presentation

This report tells the story of one of our journeys during 2018 as Sursiendo: living between the local and digital realm, we unpacked a research project-process that assessed digital security within grassroot organizations in Chiapas.

To be online is very important to most people. Also for human rights activism

According to Lori Lewis and Chadd Callahan's study (Desjardins, 2018), based on data from May 2018, per hour, more than 10.000 million emails are sent, 22 million apps are downloaded and 222 million searches are requested.

In Mexico, more than 65% of the population is online, as reported by Internet World Stats (2018).

Today, Internet is crucial in understanding how our societies operate. Internet is present in nearly all social, political, economical and cultural spheres in Mexico and in the whole world.
To be online is very important to most people. Also for human rights activism.

But beyond numbers, we believe in focusing on the people, the "whom", the "how" and the "what". How we use and relate to each other through Internet, through what devices and programs. What is at risk when we are online.

We like to think of Internet as a territory, "like the lived and heartfelt space embedded in our day-to-day", as Arturo Escobar (2010) defines it; territory as a setting of social relationships. This is why we perceive Internet as a social construct and our understanding of it implies grasping how it is produced and 'inhabited'.

But this territory, like many others, is threatened by neoliberalism, through surveillance and control, criminalization, deprivation/dispossession, data marketing and a lack of ethics

But this territory, like many others, is threatened by neoliberalism, through surveillance and control, criminalization, deprivation/dispossession, (personal) data marketing and a lack of ethics. Internet is a disputed territory.

In this sense, during 2018, we decided to perform a research related to part of this dispute: digital security in grassroot organizations of Chiapas, aiming to assess what was happening in the region.

In Mexico, digital security is at stake for organizations, activists and human right defenders, as we have seen with the deployment of State surveillance, the cases of Galileo (developed by Hacking Team) and Pegasus (by NSO Group) spy software, along with criminalization and censorship.

Public institutions, technology corporations and organized crime put at risk the safety of defense and accompaniment work towards collective processes.

Our proposal was to perform assessment, based on popular education and participatory dynamics: workshops, questionnaires, interviews and online information sheets. We plunged into the participants contexts, analyzed all this information and, finally, returned it back to the groups in a way that could help them improve their practices related to digital technologies standing on a solid foundation they could unfold in a long-term accompaniment.

Internet is a disputed territory

But, what is digital security? In some cases, it is defined as computer infrastructure protection and

everything related to this and, specially, information contained in a computer or flowing through computer networks; in others, it is defined as the practices and tools that we use as users to protect our devices, information and digital interactions.

Both definitions describe realities, but, in Sursiendo, we prefer to frame 'digital security' as digital self-defense and self-care practices that seek to improve our 'digital lives' in a (long) journey towards technological sovereignty.

Or, as some members of the organizations we worked with described: "a series of habits, tools that one uses in their daily lives in order to protect information/data" or "the possibility to move around in cyberspace/Internet without being at risk, at least not at risk if we haven't chosen to be; neither me, neither the people that surround me, neither whom I work with".

We consider the concept 'security', in itself, tricky and it has led to the state of surveillance in which we are immersed today.

It is impossible to be 100% 'safe and secure', but we can take measures to look after our digital interactions and, in consequence, look after our work as defenders and activists.

However, due to the fact that the concept of 'digital security' is now generally used to talk about these topics, we will adopt it during the whole report.

in Sursiendo, we prefer to frame 'digital security' as digital self-defense and self-care practices that seek to improve our 'digital lives' in a long journey towards technological sovereignty

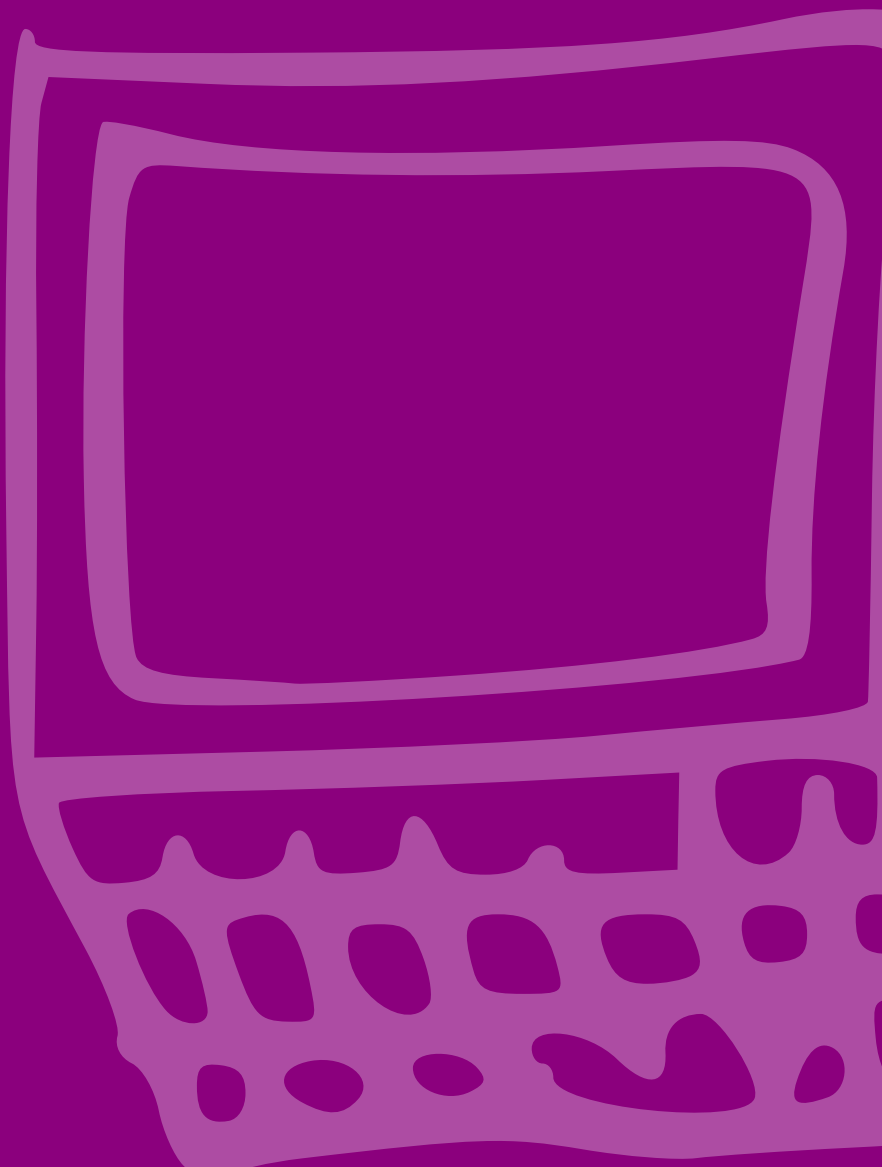
In the following pages, we synthesize what has happened in terms of digital security in Mexico and Chiapas, what findings have come up in the research and what needs and challenges emerge

This assessment process followed eight organizations in Chiapas that work in different areas: human rights, migration, womens' rights, land and territory rights, accompanying grassroot groups, communities (rural and/or indigenous) that resist against the "development extractivist model" and sustain alternatives. In order to ensure confidentiality and protect their work, we do not mention their names in this report.

In the following pages, we synthesize what has happened in terms of digital security in Mexico and Chiapas, what findings have come up in the research and what needs and challenges emerge.

We would like to thank the organizations for their participation and trust in this journey that still unravels. Also to the Human Rights Center Fray Bartolomé de las Casas (Frayba), that has shared their experience and Paola Ricaurte for her contributions to this report.

1. Context of surveillance



The sociologist and researcher David Lyon defines surveillance as "any focused, systematic and day-to-day attention to personal details for the purposes of influence, management, or control" (Bauman and Lyon, 2013).

But, in the digital era, surveillance isn't only quotidian, it is pervasive: a harvesting of information that isn't necessarily directed and focalized anymore but mainstream and generalized, implemented by State, corporations, mainly in the US and European headquarters.

One of the organization directors says: "I think that it's easy for those who want to have your data". Another participant shares: "to say 'I don't have anything to hide' is very easy, but we all have things that we don't want to be around".

Furthermore, all the data collected on digital networks tends to be stored several times, in different locations and during an indefinite period of time. Data collection, storage and analysis is an automatic process that doesn't require a great deal of effort (albeit many resources), so it's generally easier to just take it all in case in comes in hand afterwards. In addition, mainstream corporate platforms don't present transparent information on how they use the data they store. Having control over your own data isn't always possible.

"In summary, digital communication surveillance is pervasive, automatic, effective and always alive. You can encrypt communication but it's difficult to hide patterns and interrelationships" (Sparrow, 2014).

Mainstream corporate platforms don't present transparent information on how they use the data they store. Having control over your own data isn't always possible

In Mexico, there has been several cases of surveillance and criminalization through Internet; purchase and use of spying software against activists, journalists, human right defenders

1.1 A very short story about digital surveillance n Mexico

We underline the relevant words of Jorge Hernández (Frayba) in one of the interviews of this research:

"the first challenge as human right defenders is that we have to know exactly where we stand, we can't be 'innocent and naive', we can't ignore the context and the interests that we are revealing; secondly, even though the State is, in first place, accountable in protecting the work (and workers) of defending human rights, safety and security is personal, it is mine and that of my collective, without exempting the State of this responsibility. We have to take into account that we live in an oppressive State, a State that spies on us; a State that deploys fear and repression as a mean of control over the population".

In Mexico, there has been several cases of surveillance and criminalization through Internet; purchase and use of spying software against activists, journalists, human right defenders. These cases have been documented and analyzed by human rights organizations. Cases that we depict in this report, based on news and published reports.

The Constitution of Mexico acknowledges the respect of human rights. Amongst other rights, it establishes the protection of the right to privacy related to information about our private lives (about ourselves, our family, residency, documents, belongings) (Laurant and Laguna Osorio, 2014).

The Federal Institute of Information Access and Data Protection (Instituto Federal de Acceso a la Información y Protección de Datos - IFAI-) is an institution in charge of protecting individual rights in matters of data protection. Whilst the only federal law that addresses data privacy and protection held by individuals is the Federal Law on Protection of Personal Data Held by Individuals (LFPDPPP), passed by the Congress of the Union in July 2010. It's application scope includes individuals and companies, but not governments or other public entities (Laurant and Laguna Osorio, 2014). Furthermore, the Supreme Court also establishes that private communications are protected, by Constitution, from "real time" surveillance , as well as from interference of the hardware where this information is stored.

Spying is prohibited explicitly in the Constitution. There is a legal framework for the protection of personal data amongst individuals but, in terms of spying performed by government, the legal mark is lax

In summary, spying is prohibited explicitly in the Constitution. There is a legal framework for the protection of personal data amongst individuals but, in terms of spying performed by government, the legal mark is lax (Rodríguez García, 2017).

In Mexico, there isn't a specific regulation of highly intrusive surveillance tools like spy software. However, jurisdiction acknowledges the possibility that some authorities request federal judicial authorization in cases of intervening private communications for specific means (R3D, 2017).

In 2009, the Federal Telecommunication Law was modified so that telecommunication service providers have to store communication data traffic (metadata), including the type of communication,

services used, source and destination, date, hour, duration and geolocalization of the communication devices for at least 12 months.

In 2012, the Federal Telecommunication Law was modified again, establishing that telecommunication companies had to cooperate with General and State Prosecutors, providing them with real-time cellphone geolocalization without court order.

In 2013 (though published in 2014), more changes appeared that involved extending communication surveillance methods. Telecommunication service providers must store metadata for 24 months and may store them during an indefinite period of time if requested, just once, by a government authority. These changes also allow authorities beyond the penal system, like CISEN, the Army, the Navy and Federal Police to determine the real-time mobile communication geolocalization without court order, under the vague and ambiguous statement of combating crime (LFTR, 2014).

In the last years, laws, regulations and national budgets related to surveillance have gone under drastic changes. Regarding the context of the misnamed "war against narco/drug dealing" , driven by international cooperation agreements related to security such as the Merida Initiative, Mexico has experienced a series of legal reforms that allow an increase of available surveillance power and techniques for security agencies, both for crime investigation and prosecuting, as well as "national security threat" prevention.

For the international organization Article 19, these measures attempt against human rights because they lead to "mass surveillance". "They are enabling the ability to collect all our online communication data and activity without judicial control. In other words, the Army can demand our Internet provider a record of our communications. In addition, there's a platform that monitors in real-time every step we make, where we are, with whom we meet and whatever digital trace we produce", points out the organization (CNNMéxico, 2014).

The Army can demand our Internet provider a record of our communications

99% of the times, communication surveillance is illegal, according to the report by the Network in Defense of Digital Rights -Red en Defensa de los Derechos Digitales- (Pérez de Acha, 2016; R3D, 2016). The laxity of the Mexican State regarding spying hasn't changed even after the multiple documented cases and controversies related to information leaks in the news.

It is clear that (the techniques and power of) spying/surveillance is not being used to prevent "national security threats" or to stop crime or drug dealing/narco. Most of the times, they are deployed against people that question and challenge (the practice of the current) power, against human right defenders, journalists, activists, etc. In the last years, different cases of how the Mexican Government has used programs to spy on the before mentioned groups have been revealed. An essential part of this strategy has been to rule over the media with an 'iron fist' and silence critical voices, including those on Internet, and, in consequence, limit the freedom of expression.

In 2012, contracts made by the National Defense Department to hire surveillance technologies were disclosed. This equipment can monitor emails, intercept calls, voices and background noises

1.2. Government, companies and spyware

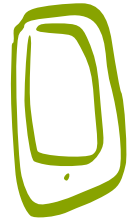
Since 2007, reports related to the cooperation between the Mexican Government and the United States -in matter of phone call and email intervention with Verint company equipment- have been published.

In 2012, contracts made by the National Defense Department to hire surveillance technologies were disclosed. This equipment can monitor emails; intercept calls, voices and background noises; capture images; extract SMS, MMS, contact lists, calendars, GPS localization and screenshots; access and manipulate system files, SIM card and hardware information, etc.

One year later, the Canadian organization Citizen Lab revealed that Finfisher spying software (by the English company Gamma International and Italian company Hacking Team) was used to spy on human right defenders, activists and journalists (Flores, 2015). At the time, Wikileaks shared with daily newspaper La Jornada information about these companies: Gamma Group and Hacking Team sent some of their members, in 2013, to Mexico. The same year, media echoed information about contracts that the Attorney General's Office made to hire spying software in 2012 (Reforma, 2013).

Between 2014 and 2016, more information came out, pointing out that "Mexico is the country that has invested more money in Hacking Team and ci-

tizen surveillance" (Lacort, 2015). This coverage detailed what institutions and state departments hired these services and how much money they had spent.



In 2017, the campaign #GobiernoEspía (Spying Government) was launched, in which Mexican organizations, with support of Citizen Lab and other media (like The New York Times) (Ahmed y Perlroth, 2017) gave evidence that Federal Mexican Government and state departments had purchased and used Pegasus sypware (by the Israeli NSO Group) against journalists, human rights defenders and activists, thus severely violating their rights.

Installing this sophisticated spy software allows the attacker to take control of different cellphone functionalities and access content and, in consequence, monitor every detail of someone's life through their phone. Despite allegations, in September 2018, Citizen Lab confirms that Pegasus software is still active in Mexico.

"There is an impressive record of our lives -including private, intimate and family-related aspects of our lives- on all possible digital means", reflects a communication lead of one of the participant organizations of the research.

Installing this sophisticated spy software allows the attacker to take control of different cellphone functionalities and access content and, in consequence, monitor every detail of someone's life through their phone

On the 8th of July 2015, Wikileaks published more than a million emails filtered by the Italian malware surveillance provider Hacking Team. The Chiapas government was included in the list of possible clients

1.3 The context of surveillance in Chapas

In 2010, Héctor Bautista, member of the libre/free software community and InfoChiapas.com site administrator was arrested by the state police, accused of child pornography. His computer and external memory devices were confiscated. Apparently, the real reason of the arrest was because of an article Héctor had published, addressing the government's debt. He was in custody for 40 days and then released (SIPAZ, 2010).

Three years later, in 2003, Gustavo Maldonado was arrested (Mariscal, 2013), accused of drug dealing. A case full of irregularities. Maldonado was critical with the Chiapas government on social media. Months before, Maldonado summoned a protest in defense of water and land rights in Tuxtla (capital city of the Chiapas state). The same evening of his arrest, Maldonado had published a video and retwitted information related to Blackeyed Hosting Monitors, surveillance equipment used to trace digital activists in Chiapas. Maldonado was released after 90 days of arrest (Robles Maloof, 2013).

On the 8th of July 2015, Wikileaks published more than a million emails filtered by the Italian malware surveillance provider Hacking Team. The Chiapas government was included in the list of possible clients (Wikileaks, 2015). However, negotiations seem to have started one year before, as mentioned in an email dated on February 2014, by a White Hat Consultors employee, a company "specialized in information security and cybersecurity, and fo-

cused on clients from the government, finance and service provider sector". In June 2015, an employee of the Mexican company Heres declares that they had established communication with two government dependencies of Chiapas related to the "security area", interested in Hacking Team's proposal and services.

The general context of violence and persecution in Chiapas has increased in the last years. And in ways that before weren't conceivable. In one of the interviews of our research, a human rights defender, with many years of experience in the State, told us with surprise: "Yes, [surveillance] is incredible right now, like science fiction. Big Brother is watching you. Everyone knows. We're discovering things that we thought weren't possible. Neither at a technological level, neither at an ethical level". Likewise, in another interview: during the actions against structural reforms, groups that work for State Security "installed a van and recorded many things; a word repeated many times catches their attention, they trace where it's coming from".

"Yes, surveillance is incredible right now, like science fiction. Big Brother is watching you. Everyone knows. We're discovering things that we thought weren't possible. Neither at a technological level, neither at an ethical level"

Also, in the last 10 years, phone intervention (both human rights defenders' personal devices like organizations' phones), criminalization, hostility, physical persecutions have increased considerably. Although, as some participants mention: "lately, I see it's not necessary to physically appear; if they do, it's because they want you to know you are being watched. But, nowadays, obviously, all this surveillance leaks into phones, email accounts, the dron that hovers above your house and you

don't even realize, satellite localization, the cameras on the streets of Tuxtla or Chamula. There is an impressive record of our lives, including private and intimate aspects of our lives and those of our family, recorded in all possible digital means".

Metadata

Communication metadata is data about an individual's communication, for example: the sender and receptor's telephone number; date, hour and duration of a communication; SIM card (IMSI) and device (IMEI) identifiers; antennae localization data generated when we connect to them through our cellphones.

Generally, metadata collection, storage and analysis is minimized, specially related to communication content. However, communication metadata can reveal as much or even more personal information than the content of communications in itself.

SOURCE: Red en Defensa de los Derechos Digitales (R3D) (2016) El estado de la Vigilancia: Fuera de control. https://r3d.mx/wp-content/uploads/R3D-edovigilancia2016.pdf

2. Research

2.1 The beginning, methodologies and assessment data analysis

We worked with eight social organizations of the State of Chiapas in this present research. The selection process criteria was based on the previous knowledge we had on the work of these organizations and the different areas of human rights each organization works with.

We worked with organizations all over Chiapas dedicated to the defense of human rights, land rights, womens' rights, migration rights, education rights, distributed in different areas of the region.

With the intention of contributing to this research, we also gained input from the Human Rights Center Fray Bartolomé de Las Casas (Frayba), that has been developing their own digital security process for the last eight years. Jorge Hernández, member of this organization, mentions that Frayba considers holistic security as part of their political standpoint because, according to their analysis: "there is no such thing as low profile human rights defenders; we all fiddle with interests that the State wants to keep untouchable; we point out things that the State doesn't want to reveal and, in this sense, all human right defenders are at risk."

"There is no such thing as low profile human rights defenders; we all fiddle with interests that the State wants to keep untouchable; we point out things that the State doesn't want to reveal and, in this sense, all human right defenders are at risk."

Throughout the assessment process, we worked with a participatory methodology and used five different research techniques in order to perform a deep analysis that allowed us to establish a sort of 'base line' of the current grassroot digital security context in Chiapas.

The main goal of this research is to gain insight on the particular needs of each participant organization so we can adapt mechanisms that foster a digital security (practices and tools) appropriation in their human rights work. As we mentioned before, even if the State is liable for ensuring human rights activism, we can't trust them to do so. This is why human right defenders assume that they have to undertake their own digital care.

The assessment is based on five information sources:
- previous research including available public information about the participant organizations and the most visible members (in total 8);
- on-site assessment workshops with participant organization members (in total 8);
- field notes we took during the workshops;
- completed questionnaires we handed out the

participant organizations about basic digital tech use and their perception on their organizational security, etc (in total 71 completed questionnaires);
- in depth interviews with some of the members of each participant organization we worked with (in total 16).

In terms of the methodology, the three main participatory tools we were inspired by were:
- Participatory Action Research (PAR) (https://en.wikipedia.org/wiki/Participatory_action_research), a community research approach that underlines implication and action. This approximation seeks to understand the world whilst transforming it, collaboratively and through reflection.
- Inform-action, tool developed by Mining Watch Canada, the Mining Conflict Observatory of Latin America (Observatorio de Conflictos Mineros de América Latina) and the Environmental Conflict Observatory of Latin America (Observatorio de Conflictos Mineros de América Latina) that addresses the different people/agents involved through data mapping.
- Digital Security Assessment for Human Rights Organizations: A guide for facilitators (Diagnósticos en seguridad digital para organizaciones de derechos humanos y derechos territoriales: un manual para facilitadores), designed by Técnicas Rudas that, based on the classic risk model, examines uses, risks and threats for organization members in the digital realm.

In terms of the methodology, the three main participatory tools we were inspired by were: participatory Action Research, inform-action, Digital Security Assessment for Human Rights Organizations

As part of this initial assessment and research phase, we decided, as an essential task, to perform workshops as a way of "returning back" research results to the organizations, along with the generosity and trust they shared with us

In different moments of this research, we used analogue methods. Data analysis was one of these moments. We believe that we "think better" on paper. For this reason, we wanted to use other technologies to combine diverse voices we gathered through the previously mentioned information sources.

One of the workshop participants mentions: "it's super interesting how we visualized the interconnections amongst us in this exercise we did with Sursiendo. Everyone is there. We are all interrelated. And everything that we use".

Finally, we would like to point out that, as part of this initial assessment and research phase, we decided, as an essential task, to perform workshops as a way of "returning back" research results to the organizations, along with the generosity and trust they shared with us. For those of us that participate in this research proposal, it is fundamental to drop out of the current extractivist model, including the information and research field where, rarely, the people subject to the research receive benefits. So, in the last part of the year, we organized these meetings where we returned back this information and put into practice some learnings that emerged in the research.

2.2 Some Findings

"We've even had to take out our personal mail accounts from our organization site", says a coordinator from one of the participant organizations from Chiapas in this assessment process. This

statement is very significant: it reveals what Internet has become for most human rights defenders and activists.

Our personal data, means of contact, location or itineraries, comments about our family, vacation photos, sensitive data about our partners, etc. can be used by people that hinder human rights work. Add to that, using insecure networks, apps that profit from our data, software easily monitored, devices that are robbed or lost: our vulnerability increases.

SENSITIVE INFORMATION TO SHIELD

"Most information is sensitive, confidential and the mechanisms we deploy are insecure and vulnerable", mentions one of the participant organi-

We have noticed a concern around surveillance that some institutions (local, state, national and international), organized crime and extractivist companies operate in the region

zation members. Furthermore, this person underlines, like other participants, that the most important information is that of the people and processes they accompany, along with personal and family data.

Broadly speaking, we have noticed a concern around surveillance that some institutions (local, state, national and international), organized crime and extractivist companies operate in the region (mines, hydroelectric power plants, etc.) Mostly in the collection of localization, family-related and personal data that puts at risk people that work in organizations and those who collaborate with them and are in their immediate surroundings. Also, there is a fear of loosing control on their data in their internal management, their organization and strategic documents related to their human rights work, accompaniment and projects.

"I know that it is all controlled by the State, that someone can use your personal data, the data you upload, identity theft and many other things. That's why I've always been careful in not uploading things, keeping them safe, trying to prevent (...) or the same information that puts me and those close to me at risk", claims one of the womens' rights defenders that participated in the assessment.

Specifically, there is a common concern around privacy violation related to communications, specially in situations of online articulation or when monitoring activities/events. For example, there is a concern of not being able to have video calls at

ease, fearing that they will be intercepted or what they say will be monitored/collected; or that third parties will access their message exchanges via Whatsapp or any similar app, both in their day-to-day but, specially when performing certain activities. The use of email, fundamental work tool for organizations, also implies known risks for human right defenders like information leaks and malware or virus infection.

Social media (like Facebook or Instagram) is also a worry due to these information leaks, information that we publish or is available to the company. Also as a source of harassment. Also browsing and searches, when we trust an almighty company like Google, through a Chrome Browser or it's search engine.

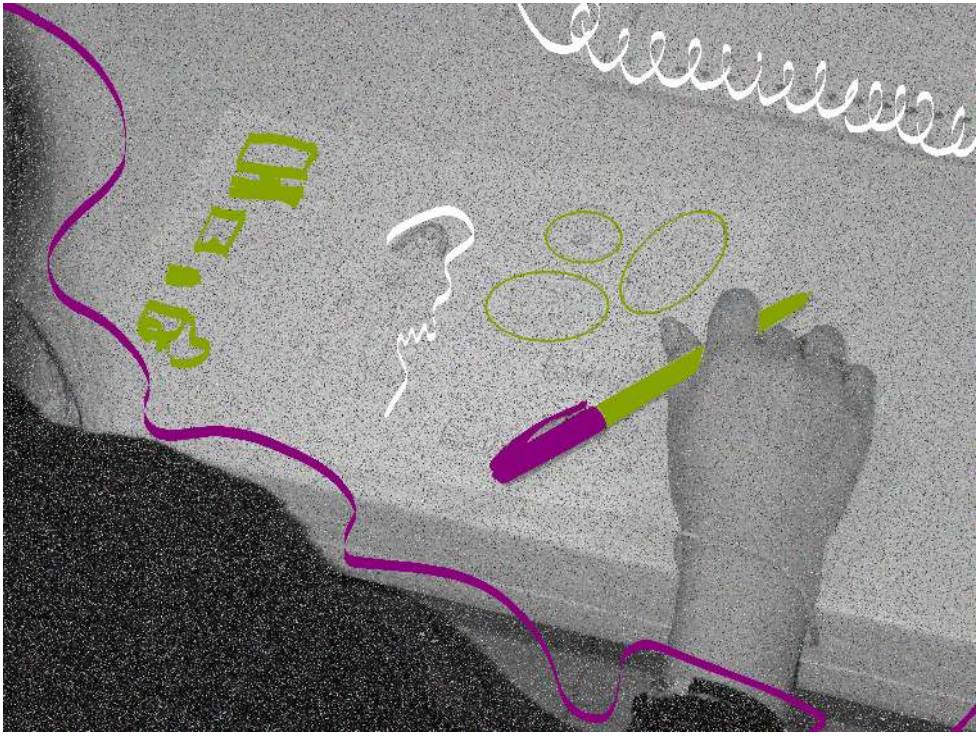
There are also concerns related to information stored on desktop computers, hard disk drives or any other device where organizations archive their work (through photos, reports, videos, records, contact lists). This information can be accessed (without consent by third parties) both via Internet or physically, which entails potential data theft that can be used or deleted afterwards. These risks hint care mechanisms we can undertake related to such information.

The use of email, fundamental work tool for organizations, also implies known risks for human right defenders like information leaks and malware or virus infection

DEVICES

In terms of digital tools used in grassroot organization work, the main devices are cellphones and computers, as expected, and, in many cases, also hard disk drives and cameras.

Thus, computers are crucial when addressing digital security. During the assessment, we found that nearly all participant organizations use desktop computers with Windows operative system (except one case that used Linux). This is the first risk factor because it is well known that Microsoft software enables information leaks (Crespo, 2016), due to flaws and the company's policies. For example, the use of 'backdoors' is common: remote non-consented server access to devices. It is also known that Microsoft has collaborated with security agencies (like the NSA), providing them with thousands of users data (Tubella, 2013). Also, Windows programs are susceptible to virus, malware and spyware.



Antivirus use isn't as generalized as we thought (no program installed or out-of-date software), neither is the use of complex passwords for device and platform service access.

Cellphones become even more relevant. They are, inherently insecure: we tend to have them on us, constantly connecting to different antennae and networks, easily lost or robbed. Users generally, for commodity, store lots of information on their smartphones and usually connect to different communication platforms. Main cellphone operative systems don't adapt much to individuals particular needs and, most of the time, we must trust blindly the apps we install (and others can't be uninstalled). These characteristics make cellphones a 'window towards the world', through which we obtain information and communicate, but also through which important data spills out without us knowing.

The recommended practice of backing up data on external hard disks is common amongst organizations. But a clear and realistic backup policy is necessary in order self/collective care conveniently. We also found that USBs are used for storage even though they are very vulnerable devices.

Cellphones become even more relevant. They are, inherently insecure: we tend to have them on us, constantly connecting to different antennae and networks, easily lost or robbed

SOFTWARE

Regarding apps and programs used, apart from the operative systems we mentioned before, we observe the constant use of commercial social media, specially Facebook; Skype (Microsoft proprietary software) videocalls; cloud storage

In the assessment workshops, participants were interested in understanding what malware actually is and what type of metadata affects our security

(via Dropbox or Google Drive); email through Gmail. All of these options are not advisory due to the fact that they are proprietary: they can't be audited and they belong to corporations that are allies of authorities. Whatsapp is another example. Also, they are more targeted by security breaches and virus as they are more mainstream and commercial.

In the assessment workshops, participants were interested in understanding what malware actually is and what type of metadata affects our security.

AGENTS/ACTORS

Amongst the organizations, the same agents tend to come up in terms of whom could be interested in the sensitive data they (the organizations) handle and could be accessed without consent.

Federal government entities (mainly attorney general's office, federal police, the Research and National Security Center -CISEN-), the Chiapas government, state police and some secretaries; local government and police forces that assist them; parapolice that tend to be tolerated (sometimes even driven and supported by) government; organized crime and drug dealing/narco groups; extractivist (mines, water extractivism, intensive agriculture, tourism, etc.) companies interested in the region. Other actions mentioned are: intelligence services, both national/Mexican -like CISEN- and international -like the CIA (USA) and Mossad (Israel)-, that have means and resources to obtain information and seek cooperation from social media platform owners.

In addition, each participant mentions local actors. In case of women rights activism, these local agents are a main threat.

Participants also point out that, in many occasions, agents are coordinated or conspire together, "police and organized crime is sometimes the same thing" or that the government's negligence (at different levels) in protecting human rights becomes part of the problem.

INCIDENTS

To wrap up these findings, we underline the security incidents that some organizations have shared with us, in many cases related to data and information. For example, noise and interference in office and personal phone lines, threats through messages or phone calls, forced entry in offices or other buildings. Also, on-site or remote surveillance in events or infiltrations in meetings, files that disappear on computers.

Slander through social media (specially on Facebook and Whatsapp chain messages). These mentioned practices infringe human rights defenders.

Finally, we want to echo comments regarding the need for funders to be more aware of digital security in order to establish safer communication with grantees and look after, in each moment, the information they share and store, and, in consequence, the processes they support. Organizations defend that digital security is holistic and collective.

In many occasions, agents are coordinated or conspire together, "police and organized crime is sometimes the same thing" or that the government's negligence (at different levels) in protecting human rights becomes part of the problem

In the context of our work with these organizations and groups we intend to follow-up, we lack enough long term exercises and appropriate tools that can help us 'measure' results. Creating these tools is, in itself, a task yet to be done.

We have found people that want to learn new tools and acquire practices that reduce the risks that emerge in their work and activism. Even though there are different levels of knowledge and experience, the intention is to make an effort and support each other, walk together in that direction.

"An agreement regarding security implies that many people are in the same channel and that is complicated. If it's already complicated to do so amongst a group, even to communicate via Telegram instead of Whatsapp; or download Signal which for many is a drag or they don't understand how to do it or they don't have enough storage on their phone... You end up using the same damn thing as always."

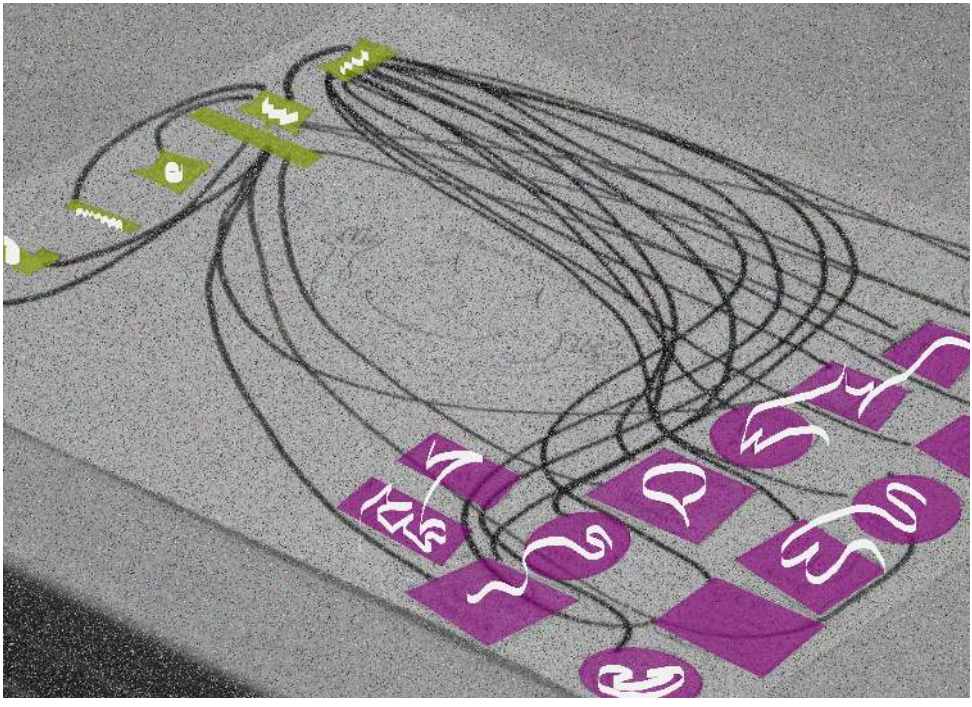
2.3 Challenges and needs

During this research journey, we have encountered big challenges. Particularly, we have ratified, by the participants themselves, the hows and whys of the need to address "digital security" within the organizations. Even though we have observed that the participant organizations are concerned about digital security, there are many challenges. Raising awareness amongst those who do not share this concern is the first step.

In itself, enabling a real long term 'appropriation' process is a challenge. In the context of our work with these organizations and groups we intend to follow-up, we lack enough long term exercises and appropriate tools that can help us 'measure' results. Creating these tools is, in itself, a task yet to be done.

Jorge Hernández, from Frayba, an organization that has already walked this walk of appropriation, tells us: "it has been a step-by-step process, 8 years. Seeking bonds with other collectives that want to support you is essential". Jorge also tells us about the relevance of capacity building tools like Moodle, tools available online so you can have a look at information when you need to, document learnings and systematize processes.

It is important to understand that guides and learning platforms are necessary in the extent that they relate to the actions and tools visualized and shared during the workshops, not as a substitute of these face-to-face moments. In this sense, having the capacity to provide 'sufficient' accompaniment in order to reduce moments of 'anxiety' and frustration on the way is indispensable.



"An accompaniment with a clear time-line, starting with simple things and taking our time is important; it would be good to specify 'deadlines' so we can realize that it needs to be in our planning route and taken seriously by the team"

Groups and organizations that do accompaniment in this field know how important the process is. In the context/framework of adopting new technologies in our digital self-defense, this characteristic entails it's own challenges.

Firstly, we stumble upon the fact of integrating 'digital security' as part of an array of 'digital security' actions/practices. In many occasions, activists and human right defenders perceive information and communication intrusion as something that can happen to others, but not to themselves.

Also, there are groups that have a lot of workload. In this sense, time management (work flows, task management) becomes relevant in order to ensure that digital security is useful at long term. We have also observed a certain rooted fear towards new technologies. Resistance towards 'the new' is very common. The perception that technologies are 'for experts' slows down the appropriation process.

If we also take into account the increase in cellphone use and the contradictory feeling of 'being at risk' and 'need' that human right defenders go through when using them, the scenario become more complex.

We include a reflection from one of the participants: "an accompaniment with a clear time-line, starting with simple things and taking our time is important; it would be good to specify 'deadlines' so we can realize that it needs to be in our planning route and taken seriously by the team".

It is also important to consider the need of creating collective agreements within the organization, agreements that come from the members and related to the practices that they acknowledge as 'insecure' and those concerning sensitive data, as well as the willingness of transformation and learning that it will imply. These agreements must be firm and gradual. They imply a certain level of commitment, on behalf of those that accompany and those who are guided.

In this phase, we prioritize 'simple' resolutions that entail transforming rooted habits and can be adopted by all members on board. We observe that the relationship person-device requires a 1:1 attention which means adapting time and efforts. Building trust in technology use is essential when enabling long term change. One must go back to the same place, repeat, again and again.

"There are things that will be short, mid and long term. Some that are precisely habits we don't have and don't perceive as necessary because we are not used to questioning them until something happens", says one of the participants.

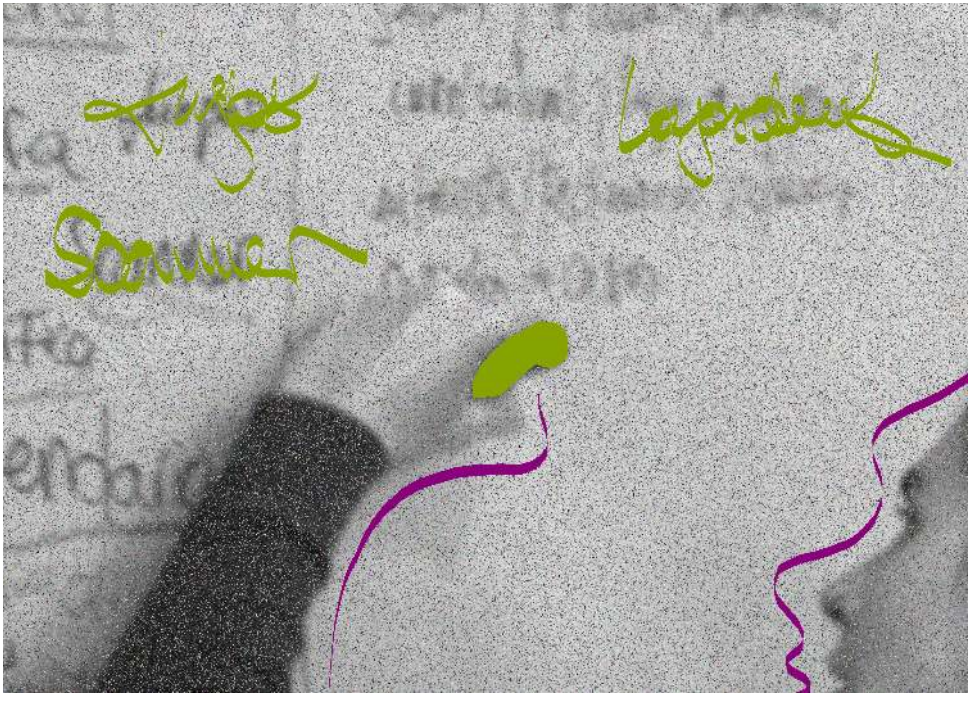
Popular education shows us to 'go at the pace of the slowest comrade'. This is an aware agreement we establish amongst all in the accompaniment. However, in practice, this implies attention, commitment, patience and a shared perception that we are still learning.

In this sense, another challenge is breaking the 'stigma' that orbits the difficulty to improve our

It is also important to consider the need of creating collective agreements, that come from he members and related to the practices that they acknowledge as 'insecure' and those concerning sensitive data, as well as the willingness of transformation and learning that it will imply

digital practices and use of operative systems and/or FLOSS software. We believe that, in order to make this a reality, we need to 'embody it', which means that each person can learn from their own experience and not just observing the errors, what is wrong, or just providing a 'technical solutionism', but also actions, gestures of mutual support where we can, together, ask ourselves, solve, manage in collective. And, of course, dismantle the still established myth that "using libre/free technologies is safer but harder".

As we mentioned before, there are different levels of knowledge related to technologies within the organizations. For some, it was their first approach to digital security. Implementation, in these cases, was significantly different to those who had already been in workshops.



We found that organizations don't have people in charge of computer/technology aspects, not even an external service provider of trust that can assess their tech equipment.

Typically, even if they have been, to a certain degree, helpful, the digital security workshops the organizations are invited to summon few members of the different organizations and cover a lot of tools and information in a short period of time. It's just an "appetizer" and, from the experience of the participants, this model doesn't manage to help them ground practices or convey this knowledge to their colleagues within their organization. The learning gets stuck, without a day-to-day application.

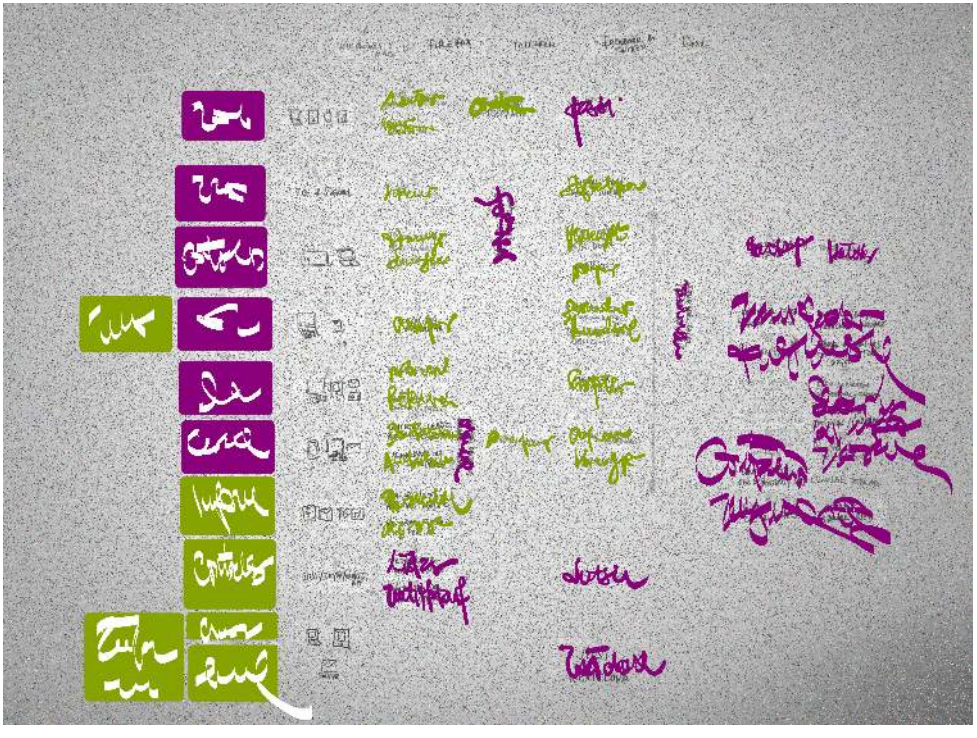
Regarding the necessary accompaniment, comments point at a more practical, simple and gradual process. Others added: "I don't like 'express' capacity building because we are slow and I think we don't grasp well (...) We go step by step. Perhaps, in a first implementation phase, we could put in practice some simple things and see how it goes and then carry on with others. In sequence. Not all at once". Participants included in the reflection the emphasis of evaluating each step in the process because, until then, the eventual workshops they had been part of hadn't taken into account some type of follow up.

Participants included in the reflection the emphasis of evaluating each step in the process because, until then, the eventual workshops they had been part of hadn't taken into account some type of follow up

On this, an internal capacity building aimed at sharing practices and tools is fundamental. Initial efforts should create baseline agreements around digital security that all participants can implement in their teams.

Not all members of the organizations handle sensitive data that require more intensive care and/or such information is centralized in one or several people. Under such circumstances, re-adapting the learning process related to each work area that the organizations needs and creating more careful information transmission and storage policies is essential.

Lastly, it's worth mentioning that some participants referred with enthusiasm to the possibility of transitioning/migrating to libre/free software: "I haven't



used it and I don't know much, but I think it's an option that aligns a lot with the discourse we have, which is, basically, a non governmental organization discourse in which we resist against certain matters. It seems cool to match discourse with action".

Jorge Hernández from Frayba also comments something on the same lines: "because of a political congruence, I mean, if we are an institution that is up for counterbalancing/going against the system and we are fattening the richest man's pocket and we don't have control over the programs we are using... That's why we decided to migrate towards libre/free software".

"Because of a political congruence, I mean, if we are an institution that is up for counterbalancing/ going against the system and we are fattening the richest man's pocket and we don't have control over the programs we are using... That's why we decided to migrate towards libre/free software"

3. Conclusions

As we have mentioned in the "Context" section of this report, Mexico has experienced several documented surveillance cases against human rights defenders, journalists and activists.

This is a good enough reason to assess digital security within grassroot organizations in Chiapas and also around digital platform data treatment that violates privacy and other rights. At present, organized civil society is aware of the situation and the need to review and address these emerging issues. "Better safe than sorry", better to anticipate any circumstance and have the knowledge and tools that foster our security and safety. Also in the digital realm.

In this research we worked, based on participatory methodologies, with eight organizations with acknowledged trajectory in Chiapas. It was very nurturing for us to share this mutual learning path which, in some cases, will evolve into a more personalized accompaniment.

We have witnessed that holistic security is part of these organizations' work. In their activism and pursuit of defending the respect of fundamental rights, many times they are at risk. Their are agents/actors that hinder and violate these rights, some of them we know well. For these reasons, organizations want to adopt digital self-care in their practices. Furthermore, putting emphasis on the political discussion of digital security is essential in order to translate it to a collective practice in civil society.

Putting emphasis on the political discussion of digital security is essential in order to translate it to a collective practice in civil society

As we claimed some months ago on this topic:

"We are interested in doing it from a collective rights perspective. The people whom we work with expect us to, apart from help with technical problems, understand the problems that emerge in their activism and talk to them in languages that are closer to them. We need to create languages as a common ground [because no, they are not invented: there is still a huge gap between front line defenders language and those who defend the territory of Internet]... Let's try the self-defense and technological sovereignty perspective from a collective creation of answers we need. The people that seek us for support, assistance in problems related to surveillance, harassment or intimidation expect us to guide them [also] with tenderness" (Sursiendo, 2018)

"We are interested in doing it from a collective rights perspective. The people whom we work with expect us to, apart from help with technical problems, understand the problems that emerge in their activism and talk to them in languages that are closer to them"

This assessment is a milestone in raising awareness about the threats, the actors/agents involved, the practices we deploy and the digital tools we use. Adopting new routines and software isn't an immediate process. The difference lays in the ways we transit these processes of use and appropriation. "there's an emerging approach of working with technologies from a social perspective that touches people, that goes to where they are. Through inhabiting these spaces, we can break with the idea that 'inclusion' means 'bringing' people to our spot, our lens, our ways of doing tech; and understand that inclusion is multi-directional". (Sursiendo, 2018)

Grassroot organizations ask us to focus our accompaniment, offer more time, walk little by little,

starting with the basics. Those whom work in this area should do accompaniment as a slow and constant process, towards all organization members, adapting to their needs, with support material and asking for commitment on the organizations behalf, creating firm and long term agreements. It's been and still is a great opportunity to learn and also a challenge.

We will continue to defend collective digital rights and fight for this Internet territory, so it can become more open, free, inclusive and biodiverse. Cheers.

We will continue to defend collective digital rights and fight for this Internet territory, so it can become more open, free, inclusive and biodiverse

4. References

Ahmed, Azam y Perlroth, Nicole (2017) 'Somos los nuevos enemigos del Estado': el espionaje a activistas y periodistas en México. New York Times.
https://www.nytimes.com/es/2017/06/19/mexico-pegasus-nso-group-espionaje/

Aristegui Noticias (2012) Gobierno federal vía Sedena compró 5 mil mdp en equipo para espionaje, 16 de Julio de 2012.
https://aristeguinoticias.com/1607/mexico/gobierno-federal-via-sedena-compro-5-mil-mdp-en-equipo-para-espionaje/

Bauman, Zygmunt y Lyon, David (2013) Vigilancia líquida. Paidós

CNNMéxico (2014) 20 puntos clave en las nuevas leyes sobre Telecomunicaciones. Revista Expansión, 9 de julio de 2014.
https://expansion.mx/nacional/2014/07/09/20-puntos-clave-en-las-nuevas-leyes-sobre-telecomunicaciones

Crespo, Adrián (2016) Snowden se muestra atemorizado de las puertas traseras existentes en los productos de Microsoft (23 marzo, 2016)
https://www.redeszone.net/2016/03/23/snowden-se-muestra-atemorizado-las-puertas-traseras-exitentes-los-productos-microsoft/

Desjardins, Jeff (2018) What Happens in an Internet Minute in 2018?
http://www.visualcapitalist.com/internet-minute-2018/

Escobar, Arturo. 2010. Territorios de diferencia. Lugar movimientos vida redes. Envión Ediciones.

Flores, Pepe (2015) FinFisher en México: Sonríe, te siguen espiando. Informe.

https://www.digitalrightslac.net/es/finfisher-en-mexico-sonrie-te-siguen-espiando/

Internet World Stats (2018) Internet Usage and Population. https://www.internetworldstats.com/stats12.htm

Lacort, Javier (2015) México es el país que más gastó en Hacking Team para espiar a sus ciudadanos. Hipertextual, Jul 7, 2015
https://hipertextual.com/2015/07/hacking-team-mexico

Laurant, Cédric y Laguna Osorio, Monserrat (2014) El caso FinFisher. Reporte Mexico de la organización SonTusDatos para Global Information Society Watch.
https://www.giswatch.org/hu/node/4955

Ley Federal de Telecomunicaciones y Radiodifusión (LFTR) (2014)
http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR_150618.pdf

Mariscal, Ángeles (2013) Gumalo, activista de las redes sociales, enfrentará juicio en libertad. En Chiapas Paralelo.
https://www.chiapasparalelo.com/noticias/chiapas/2013/11/gumalo-activista-de-las-redes-sociales-enfrentara-juicio-en-libertad/

Miguel, Pedro y Molina, Tania (2013) Empresas de espionaje cibernético buscan ampliar mercado en México. Periódico La Jornada, 5 de septiembre de 2013, p. 4.
https://www.jornada.unam.mx/2013/09/05/politica/004n1pol

Pérez de Acha, Gisela (2016) El Foro de Gobernanza de Internet en un país autoritario (08 de diciembre, 2016)

https://www.derechosdigitales.org/10695/el-foro-de-gobernanza-de-internet-en-un-pais-autoritario/

Red en Defensa de los Derechos Digitales (R3D) (2016) El estado de la vigilancia fuera de control.
https://r3d.mx/wp-content/uploads/R3D-edovigilancia2016.pdf

Red en Defensa de los Derechos Digitales (R3D) (2017) Gobierno Espía. Vigilancia sistemática a periodistas y defensores de derechos humanos en México.
https://r3d.mx/2017/06/19/gobierno-espia/

Reforma (2013) Derrocha la PGR en equipo espía. 06-Jul-2013
https://hemerotecalibre.reforma.com/20130706/interactiva/RNAC20130706-005.JPG&text=Hacking+Team&tit=Derrocha%20la%20PGR%20en%20equipo%20esp%EDa

Robles Maloof, Jesús (2013) 90 días. Gustavo, libre. Revista electrónica Sin Embargo (noviembre 12, 2013)
https://www.sinembargo.mx/12-11-2013/3018980

Rodríguez García, Arturo (2017) El caso Maloof y el software malicioso FinFisher. Revista Proceso.
https://www.proceso.com.mx/491735/caso-maloof-software-malicioso-finfisher

SIPAZ (2010) Chiapas: Denuncia de persecuciones a periodistas.
https://sipaz.wordpress.com/2010/11/17/chiapas-periodista-teme-por-su-integridad/

Sparrow, Elijah (2014) Vigilancia digital. Reporte de LEAP Encryption Access Project.
https://giswatch.org/es/thematic-report/communications-surveillance/vigilancia-digital

Sursiendo (2018) ¿Por qué pensar en soluciones 'low-tech'? Blog Sursiendo (mayo de 2018).
https://sursiendo.com/blog/2018/05/por-que-pensar-en-soluciones-low-tech/

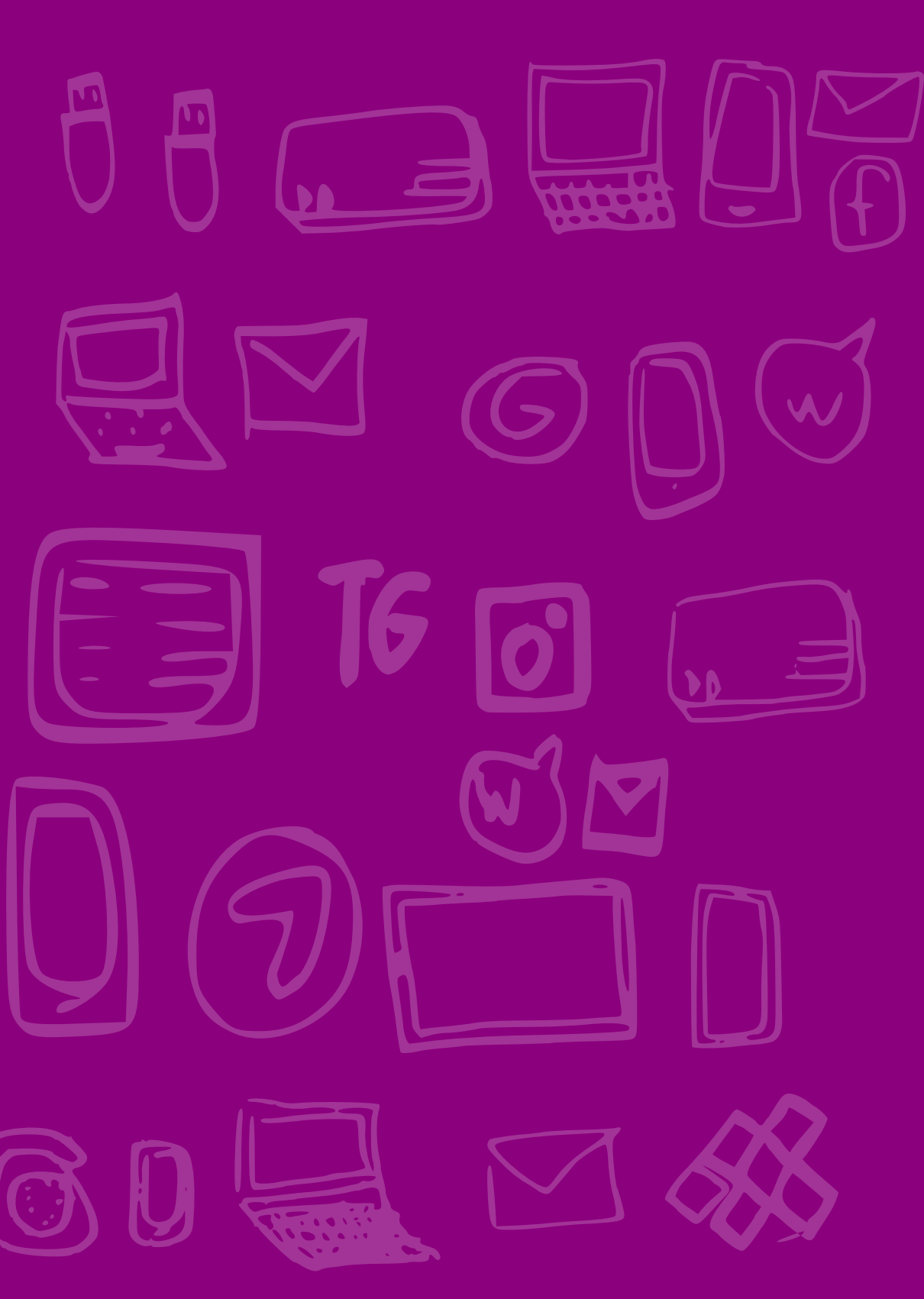
Tubella, Patricia (2013) La NSA pagó millones a los gigantes de Internet por colaborar en el espionaje. El País, 23 de agosto de 2013.
https://elpais.com/internacional/2013/08/23/actualidad/1377272049_738995.html

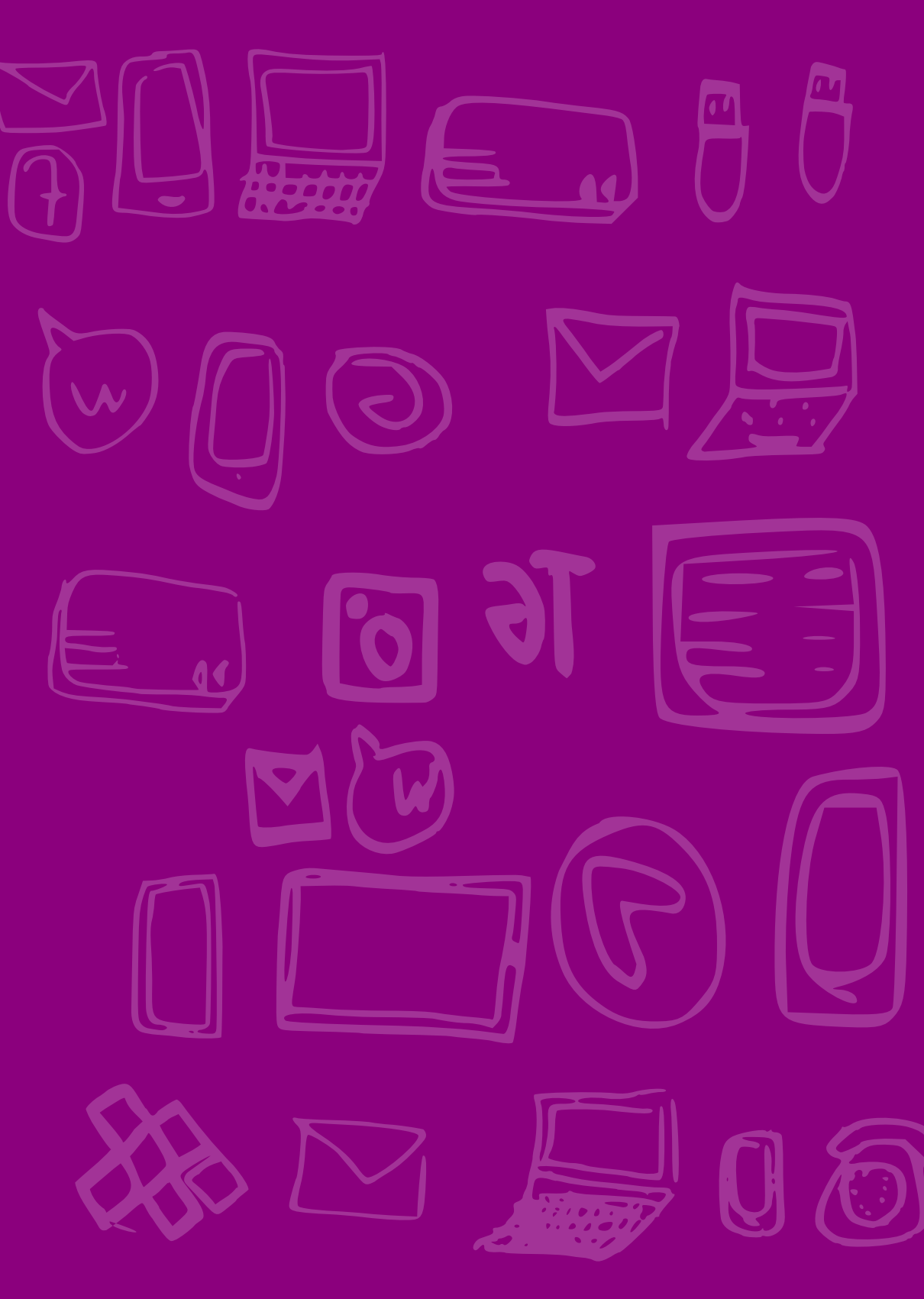
Wikileaks (2015) Hacking Team. Resultados de la búsqueda 'Chiapas'.
https://wikileaks.org/hackingteam/emails/?q=chiapas&mfrom=&mto=&title=&notitle=&date=&nofrom=&noto=&count=50&sort=0#searchresult

Wikipedia (s/f) Investigación-Acción participativa
https://es.wikipedia.org/wiki/Investigaci%C3%B3n-Acci%C3%B3n_participativa

This report was made and designed with free software:
LibreOffice, Inkscape, Gimp, Scribus and Krita.
The free fonts "Abel" were used in 12 points for the body of the text and "Gloria Hallelujah" in 14 points for the titles.

This report was printed in La Cosecha, January 2019.
San Cristóbal de Las Casas, Chiapas, Mexico.





Comunicación
Cultura Digital