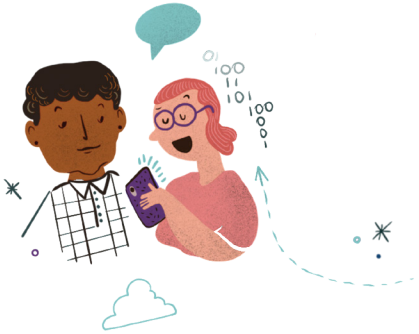
Feminist
Digital Self-Care
manual



akãhatã

equipo de trabajo en sexualidades y géneros

When thought of collectively, digital self-care works like a shield of EMPATHY:

by taking care of ourselves
we take care of others.

introduction

This feminist digital self-care manual is centered on collective action. We recognize that digital security hinges on our willingness to care for others. Thus, the methods to keep ourselves safe must be conceived from a place of collective empathy. Thinking collectively lends strength to each action that stems from our own individualities and identities.

This manual calls itself feminist because it recognizes gender inequality as a given and acknowledges that its violence is structural in nature. In other words, it works similarly to racism, ableism and other forms of oppression that are reproduced in the digital world.

Considering that normative language is unable to capture all identities that go beyond the gender binary, we have opted for inclusive language to challenge the norm. We use they/them, their/theirs because we recognize that a plurality of identities are erased when the universal masculine is used, or which simply do not fall within the binary.

» What is this manual about?

This manual is a basic introduction to different practices of digital self-care from a feminist and collective perspective. It contains our thoughts on how to carry out actions of mutual care and includes tools to accompany such practices.

» Key terms and concepts

_Risk
The possibility of suffering harm that may affect me and/or my collective. This possibility is contingent on my level of vulnerability. The basic formula for risk is the following:

$$\text{Risk} = \frac{\text{Threat} \times \text{Vulnerability}}{\text{Response capacity}}$$

_Threat
Any phenomen, person or process that may constitute a risk.

_Vulnerability
Our capacity (high or low) to face risks or events that may arise.

_Privacy
The sphere of an individual's personal life that is developed in non-public spaces. Privacy is a human right.

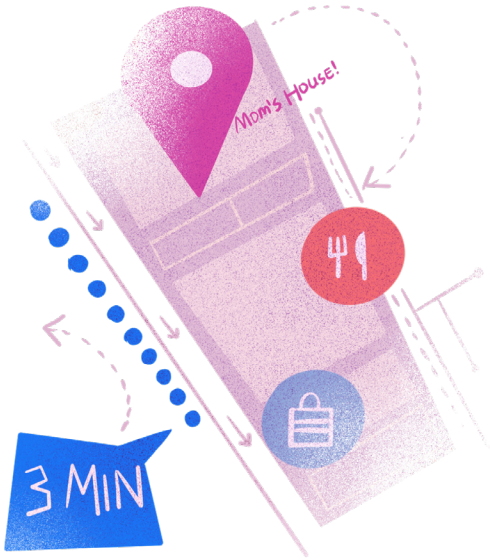
_Personal data
All information that can be connected to us and which identifies us or makes us identifiable.

_Digital rights
Those rights that allow people to access, use, create and publish content on the internet; as well as to access and use computers, other electronic devices and communications' networks[1].

1 | What are digital rights?

_Metadata
It refers to the data and the characteristics that make up our data. For example, the metadata of a picture is made up of the location where it was taken, the type of phone used to take it, etc.

_Hacking
The use of technology to crack private information with the aims of harming a person or organization. An example of hacking directed at an organization might involve its social media accounts: for example by publishing in your organization's name or deleting its publication history. In the latter case, the direct risk is losing the records of your organization's achievements.



_Encryption
The process of coding data, documents or files to make their content undecipherable and exclusively accessible with a key.

_PGP Key
Pretty Good Privacy is an email encryption protocol. Although PGP is not open source, standard OpenPGO may be used.

context, risks and threats

When we analyze technology as a process, we can better understand that every technology in our lives is the product of specifically situated interests. For instance, the interests of powerful states that develop mechanisms of population surveillance. They may also be the product of specific time periods, such as pandemics, when the tracking of persons and the indiscriminate use of personal data increases.

As part of our respective activisms, it is important to approach these technologies critically and to be creative in finding ways to use them to our benefit. The same technology that may constitute a threat to our identities and work and be repurposed and adapted in a collaborative and participatory manner. Strategic appropriation of different technologies may, potentially, increase our capabilities and the reach of our voices.

» Risk and threat assessment

Which risks and threats do we face in the framework of our activism?

Activist work is never risk free. In order to mitigate risk, it is thus important to learn how to detect it. Risks may be external to our collectives, for example, government surveillance; or they may be internal, such as the infiltration of persons. Certain risks can start out being minor, such as the hacking of an account or digital profile, but become more dangerous when the information or data our collective holds is of a sensitive nature or contains personal data.

These risks may result in:

_ The loss of our personal data, the data of our collectives, or that of our fellow activists.

_ Obstructing or impeding any of our collectives' planned actions.

_ Threats to the physical integrity of persons and devices.

» Potential sources of attack

Who are our potential adversaries? Our adversaries, one would think, are powerful entities and beings situated above us: public institutions and governments, religious organizations, fascist and anti-rights groups. However, our potential adversaries may be much closer. Our partners, family members and even our friends may all be potential adversaries.

Surveillance, harassment and persecution are not necessarily carried out top down, that is, from an institution towards our digital personas or physical bodies. Rather, they may also occur between peers, that is, in horizontal relationships. A partner or fellow activist may engage in violence or surveillance when asking for your passwords or demanding proof of location.

why we need feminist self-care

» What is collective feminist self-care?

Digital self-care is how we translate physical, emotional and psychological care to the digital sphere. This implies rethinking these practices, identifying them, understanding how they are performed as well as who makes up our care networks.

Self-care can be considered feminist when it is collective, emancipatory and transformative of traditional gender roles and oppression forms. The feminist version of self-care also needs to acknowledge that lived oppression and violence intersects with other vectors such as disability, race, sexual orientation, etc. Collective digital self-care implies protecting each other from a place of empathy, recognizing that by taking care of each other, we also take care of ourselves.

The different dimensions of digital self-care are bound with and run in parallel to our forms of physical care. By taking greater control of the devices with which we connect our reality to the digital world, we not only protect ourselves, but also others. The actions we take in the physical world, such as transporting our mobile devices or taking pictures, may render the privacy of our digital identities, and those of other people, more vulnerable to threats.

For example:

_ By not leaving our computers or mobile devices unlocked or open in public spaces
→ We make it more difficult for others to gain access to our accounts or profiles.

_ By giving our computers and mobile devices a safe password
→ We protect our accounts and sessions in case of theft.

Map of organizations that support digital care in the region

_Mexico
. SocialTic
. La Clika
. La Sandía Digital
. Codeando México
. Luchadoras
. Rancho Electrónico
. Colectivo Disonancia
. Colectiva Mecha
. SeguDigital
. Vita Activa

_Guatemala
. CiberfeministasGT

_El Salvador
. Las Mélidas

_Nicaragua
. La quimera feminista
. Enredadas por el arte y la tecnología

_Costa Rica
. Sula Batsu
. Fundación Acceso

_Panama
. Ipandetec

_Brasil
. Cl4ndestina
. Coding Rights
. Maria Lab

_Colombia
. Fondo de Acción Urgente Latinoamericano
. Fundación Karisma

_Ecuador
. Taller comunicación mujer

_Peru
. Hiperderecho

_Bolivia
. Nodo Común
. Internet Bolivia

_Paraguay
. TEDIC

_Chile
. Proyecto Aurora de Amaranta

_Argentina
. Activismo feminista digital
. Las de Sistemas
. Chicas Poderosas

_ Regional – Global

. Derechos Digitales
. Dominemos las TIC
. Access Now
. Código Sur
. Surveillance Self-defense
. Digital Defenders
. Frontline Defenders
. Ciberseguras
. Tactical Tech
. Escuelafeminista.red
. Acoso en línea
. Asuntos del Sur - SISA
. Asociación para la Comunicación Progresiva

a guide to our toolbox

» Tools

Safe passwords

Keeping our passwords safe is a key element in the good care of our digital identities. Following a few simple steps suffices to achieve this:

_ Do not use the same password for more than one account.

_ Learn about password managers such as KeepassXC to keep track of all your passwords.

» *A password manager* is a vault where you can store all your passwords under one master key. If you're not feeling creative, it also helps you generate safe passwords to use in your accounts.

» KeepassXC works with Linux, Windows and Mac.

» For mobile devices:

- Android: KeePassDX and KeePass2Android.
- iOS: Strongbox and KeePassium.

_ Create passwords that use special characters such as periods, commas, exclamation or question marks and even spaces.

_ Never leave an account password-free. Only love should be free!

Self-assessment regarding safe passwords:

◊ Are my devices protected with passwords containing alphanumeric characters?

◊ Do I periodically update my passwords?

◊ Do I use different passwords for my accounts and my organization's accounts?

Safe browsing

There are many ways to safely browse the internet. That is, with a low level of exposure to risks or attacks. There is a difference, however, between safe browsing and private or incognito browsing.

Safe browsing entails taking practical steps such as not accessing sites of dubious origin or which raise suspicion. *You can check in the address bar whether after the http there is an "s". This means that the website has a security certificate* (Secure Sockets Layer). You can check whether the address you're browsing, or the URL, is real. For example: https://www.nytimes.com/ and not a shady URL such as http://www.newyorktimes.info. Always check the trustworthiness of links before clicking or providing any sort of personal data.

There are tools such as VPNs and browsers such as TOR that provide **an extra layer of security and anonymity while browsing.** Here is an example of how they work:

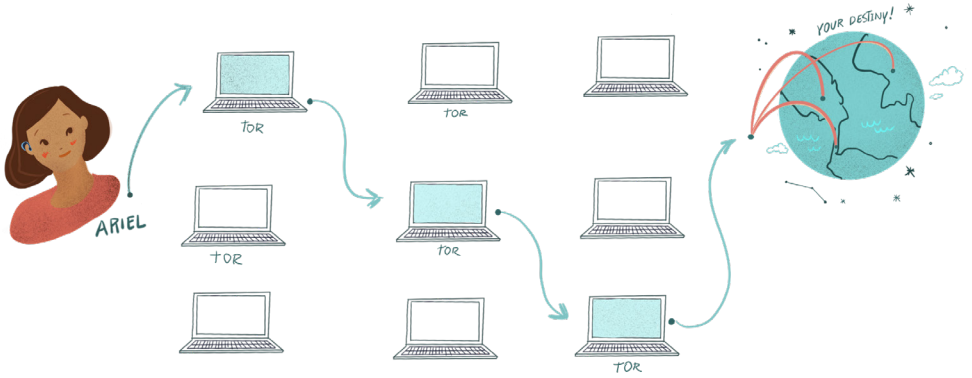
_VPN: a VPN or virtual private network connects your device through a secure tunnel to a remote server in a country of your choice. This masks your IP address, making it appear as though you are accessing the internet from the location of the remote server instead of your actual location.

· **Linux, Mac, Windows, iOS, Android / Bitmask:** https://bitmask.net/en

· **Linux, Mac, Windows, Android / RiseUp VPN:** https://riseup.net/en/vpn

· **iOS: / OpenVPN**

_TOR: The Onion Router (TOR) is free software that disguises your identity by encrypting your traffic and routing it through a series of volunteer-operated servers, known as nodes.



Which one is better? They each fulfill different functions.
Most VPNs offer end-to-end encryption, privacy and make your data 100% invisible to hackers and spies.

Unless you're using Tor's operating system, it only protects data that's transmitted through your browser. A VPN will encrypt all of the data that's traveling over your connection[2].

2 | Definitions of VPN and TOR by

You may also browse anonymously through the use of *incognito tabs* (Chrome) or *private tabs* (Firefox). This type of browsing is recommended when you are not using your own devices, for example when you are on a public computer. When you browse with these tabs, your data is not stored. This does not mean that the sites you visit won't be able to detect that you have accessed them, but rather that the device will not store this information.

Combined recommendation: use Firefox because it is a free open source browser. In addition, it uses up less memory than Chrome which makes it faster. Use DuckDuckGo[3] as a search engine since it does not collect personal data when searches are conducted. Accordingly, it does not create a profile of your preferences, it merely shows the information relevant to your search.

3 | DuckDuckGo

Self-assessment regarding safe browsing:

◊ Do I log off my accounts when I access them from devices that are not mine?

◊ Do I use incognito or private tabs when I browse on devices that are not mine?

◊ Do I use safe browsers in order to avoid leaving traces of my preferences in the browsers?

Safe messaging and communications

Safe messaging is made up of two components: one is technical and the other related to the user's behavior. There are different strategies that we can adopt to communicate more safely despite not having a safe app.

The safest app is Signal because it offers end-to-end encryption on all your conversations, including group chats. This means that your communications may not be intercepted, not even by Signal. It also offers the possibility to lock the app with a password.

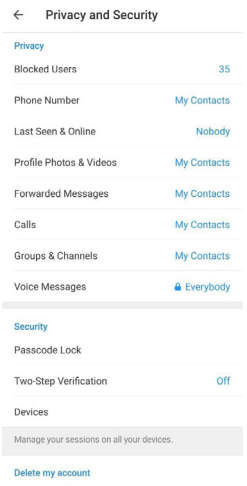
If your access to the internet is limited, your device is low on storage space and your only alternative is Whatsapp or another risky app, it is important to learn how to use them safely. These are our recommendations:

_ **Don't use a profile picture taken in intimate settings**, with persons who are close to you, family members or minors. Avoid leaving clues to identify you by.

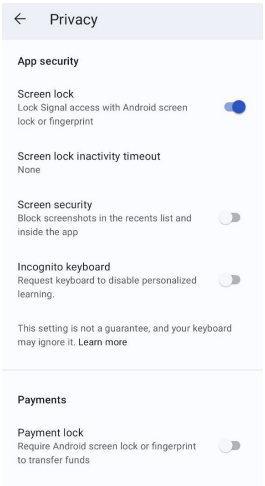
_ **Avoid using your real name on the app.** Use creative synonyms instead.

_ **Use a password to access the app.** In the Whatsapp settings you can set a password and pin to access the app.

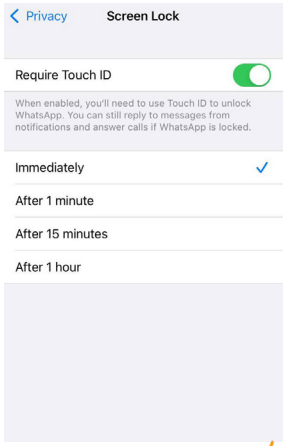
Telegram

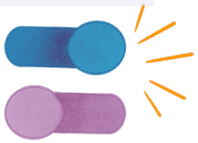


Signal



Whatsapp





If you need to share a password or other sensitive information, there are safe protocols you can follow. For example, share the last three digits of a password, followed by the first three and lastly by the three middle digits.

The table below is useful to understand how the three most popular messaging apps work[4].

	Whatsapp	Telegram	Signal
Two-step verification	✓	✓	✓
App locking	✓ * with a fingerprint	✓ * with a passcode and also with a fingerprint option	✓ * with a fingerprint and passcode
End-to-end encryption	✓	✓	✓
Requiring access to contacts	✓	✕	✕
Screenshot blocking	✕	✓ * only in secret chats	✓
Ephemeral messages	✓	✓ * only in secret chats	✓
Self-destructing messages	✓ * ephemeral messages may be forwarded or backed up	✓ * only in secret chat	✓
App locking on a device	✓	✓	✓
Content forwarding	✓ * with no mention of sender	✓ * with an option to make no mention of sender	✓ * with no mention of sender
Third-party data sharing	✓	✓	✕
Reporting tools and blocking of contacts or groups	✓	✓ * including stickers	✓

To report abuse on messaging platforms[5]

4 | Signal vs Telegram vs WhatsApp

/ WhatsApp: follow these steps to report a group chat or contact: https://faq.whatsapp.com/21197244/#Report

/ Telegram: you can report a contact, group or channel from options within the app. For stickers or bots send an email to abuse@telegram.org. Make sure to include the link and @username that you wish to report.

/ Signal: you can block a phone number, contact or group.

5 | To report abuse

For safe video calls or online meetings, you may use Jitsi (https://meet.jit.si/). This platform is open source, does not require you to create an account, nor to download an app on your computer (only on mobile devices). You can add password protection, blur the background, share screens, live stream, etc.

An option for safe emailing consists in the encryption of messages and the use of encryption keys. A fast and effective version of this is Mailvelope (https://www.mailvelope.com/). This software is open source and offers end-to-end encryption on email traffic inside of a web browser. It can be integrated into email apps such as Outlook or Gmail.

Another option is to create safe email accounts, for example on ProtonMail or Riseup Email.

Self-assessment on safe messaging:

- ◊ Do I use safe apps with end-to-end encryption?
- ◊ Do I refrain from sending passwords and other sensitive content on high-risk messaging platforms?
- ◊ Do I use pseudonyms on my messaging apps?
- ◊ During video calls, do I make sure to protect the information of other persons? For example, by not having pictures in the background.

Sharing contents and documents safely and collaboratively

When we share content, information may be filtered - the data of the transmitter and/or that of the recipient. One of the first steps we should take before sending documents or content is to erase the metadata. If the document is intercepted, it will not yield information to identify places, persons or devices. **SendReduced,** an app for Android, may be used to reduce risk when sending pictures. *For iPhones* the following steps can be followed: open the app, select the pictures to be sent, press the settings icon in the lower left hand corner and select "erase all metadata".

To send documents safely and more privately (including the option of sending self-destructing messages), the following Rise Up services may be used:

- **pad.riseup.net** – real time collaborative text editing with programmed self-destruction
- **share.riseup.net** – file uploads (pastebin and imagebin)

On sexting: if we want to practice safe sexting or the exchange of messages with erotic content, we recommend using stickers to cover your face or any body markings that make you identifiable. We also recommend using messaging platforms that have the option of sending self-destructing messages (like Telegram or Signal) and which block recipients from taking screenshots or forwarding content.

* ***Please keep in mind:*** if your information is shared without your consent - **that is not your fault!** There are organizations that can help you remove content from platforms where your files might be filtered. One of these support networks is Access Now or Acoso.Online, a digital rights organization.

Self-assessment regarding the safe sharing of content:

- ◊ Do I share content and documents using safe platforms?
- ◊ Do I download documents of dubious origins or from persons I don't know?
- ◊ Do I only download apps from safe sites such as the Apple Store or Google Play?
- ◊ Do I use a metadata remover tool?

Safe social media use

Social media, whether Facebook, TikTok, Instagram, Twitter or Pinterest, are designed to provide places to "meet" other persons who interest us, and to engage with the things, activities and topics we are passionate about. However, we need to know that **these networks feed on our behavioral patterns and learn from them.** What does this mean? For instance, if we press *like* on many dog videos, it is quite likely that our social media networks will only show us more dog videos or dog friendly content. What's wrong with that? Nothing. Dogs are great! However, when it comes to the political sphere or the sphere of our activism, social media networks can become resonance chambers for our own interests, skewing our experience and giving us a biased outlook. There is no formula to fully counteract these algorithms or to stop these networks from learning from our behavioral patterns. However, there are ways to be more aware of our social media use.

From the perspective of *collective digital care*, it is important to remember that social media networks are private companies that seek material benefit and look after their own interests. Accordingly, they update their terms and conditions constantly. A good rule of thumb is to always read carefully before pressing "ok" or "accept". *Often, social media platforms update privacy provisions that affect the security of our profiles.* Regularly reviewing these conditions is imperative to exercise self-care on social media.

Issues to consider when using the most popular social media networks

	FB	IG	TW	TK
Ability to use a pseudonym	✗	✓	✓	✓
Ability to change your username	✗	✓	✓	✓
Ability to state your pronouns or gender	✓	✓	✓	✓
Two-factor authentication when starting a session on the app or on the web.	✓	✓	✓	✓
Ability to create a private profile	✓	✓	✓	✓
Security settings for your posts (who can see your post, who may comment)	✓	✓	✓	✓
Ephemeral messaging (timed self-deletion of messages)	✗	✓	✗	✗
Security settings for message reception (to only receive messages from people you follow or who follow you)	✓	✓	✓	✓
Ability to disable location services	✓	✓	✓	✓
Ability to check posts where you are tagged before they are published on your profile	✓	✓	✗	✗

FB: Facebook **IG:** Instagram **TW:** Twitter **TK:** TikTok

Self-assessment regarding safe social media use:

- ◊ Do I check the security settings on all social networks where I have a username or my organization has an account?
- ◊ Do I know how to report attacks on social media?
- ◊ Do I have security protocols in place and do I update the privacy settings on my social media accounts and those of my organization?
- ◊ Do I use the same password on more than one social media account?
- ◊ Do I upload pictures and content without following privacy protocols, thereby exposing my fellow activists?

Digital detox

"Digital detox" is the name we give to those individual or collective practices that help us unplug from our digital identities in order to safeguard our mental, emotional or physical health.

Digital detox may be as simple as muting notifications on our mobile devices, not checking our email on weekends or even changing the screen on our phone to black and white to reduce usage stimuli.

Many apps, from their very conception and design, use patterns to "hook us"[6].That is, to make a particular technology more persuasive in its usage dynamics. We should therefore be aware of the uses we give to our apps. Technology is not neutral, it has been designed to capture our attention.

6 | Persuasive technology

Self-assessment

- ◊ Do I recognize the digital risks that affect me and my organization or collective?
- ◊ Do I follow the steps and practices of collective digital self-care when I plan my organization or collective's activities?
- ◊ Do I find moments during the day to unplug from the digital world and to root myself in my tangible present?
- ◊ Do I adopt technologies aware of the risks they may pose to my organization, myself and my fellow activists?

A digital self-care mantra to repeat on a daily basis

»The digital is real«.

Feminist self-care is collective, political, transformative and empowering.

conclusions

Our aim with this manual was to rethink the notion of digital security and to transform it into a feminist tool for self-care. Acknowledging the realness of the digital world implies acknowledging that the harassment, abuse and violence reproduced in cyberspace are also real. Digital violence is not immune to the cis(sexist), racist, classist, ableist and heteronormative logics that permeate the tangible world. This is why we insist on deploying the strategies we've built - drawing on different feminisms - to safeguard our bodies, collectives and activism on the internet. Feminist self-care, as a mechanism of digital self-defense, is a way of arming ourselves against the systematic violence that endangers us on the internet.

Keeping each other safe is a feminist policy of collective care.
The idea of the collective is central in generating these strategies of digital self-care. If feminist self-care entails a series of historic political reappropriations, the use we make of digital tools also constitutes subversive reappropriation. We can use and transform virtual platforms even when they operate as spaces that reproduce violence against historically violated bodies. At the same time as technology reproduces the well-trodden paths of violence, we may reconfigure these to broaden our room for agency.

There is an increasing number of activists and collectives that use different technologies to organize themselves, inform others, as well as to denounce violations and claim rights. There is an increasing number of social movements that inhabit cyberspace disruptively. That is, to deploy strategies of change. However, the internet is not risk free and the lives of activists can come in harm's way. This is why we seek to generate networks that democratize the use of technologies, while at the same time reducing the risk endured by those of us who have chosen to inhabit the digital world in our pursuit of social transformation. This manual, in and of itself, is an example of feminist self-care because we believe that taking care of the self is impossible without taking care of others.

As hostile attacks of fascist and anti-rights groups move to virtual platforms, new forms of spreading hate speech, threats and other forms of digital violence emerge. It is therefore important to come up with tools to mitigate the effects of digital vulnerability. Reducing risk when using the internet helps to broaden the reach of all those actions that we activists take online. In this sense, the version of feminist digital self-care we advance is a means to connect the virtual world with transformations taking place offline.

To conclude, here are some points we consider essential to strengthen feminist digital self-care:

_ Be aware of the origins of the technologies we use and the means at our disposal to transform their usage. It is possible to adapt the use of digital tools to our benefit!

_ The apps and platforms we use are constantly being updated. This is why we need to periodically review which changes may affect our safety and privacy as well as those of my collective. Assess your practices periodically. You may use the following checklists: https://protege.la/checklists/

_ Think of others from a place of empathy. Reflect on how they may be affected by the use we give to some technology or digital medium.

_ No practice of digital care is infallible. That's why it's necessary to follow a series of practices that, together, shield us and allow us to take care of ourselves and of others.

_ Don't be afraid to try out new tools but be aware of their limitations and risks. Contact fellow activists who are knowledgeable on the use of these technologies and always seek a second opinion.

acknowledgments

This manual is a compendium of lessons we have learned collectively and individually as well as a digest of the knowledge and expertise generated by a series of organizations working for the defense of digital rights in Latin America.
[Refer to the map to learn more about them].

Gracias a todas las personas involucradas para desarrollar este material.

» *Artwork:*
Lu Sánchez – Costa Rica

» *Layout:*
Cristiana Castellón – Nicaragua

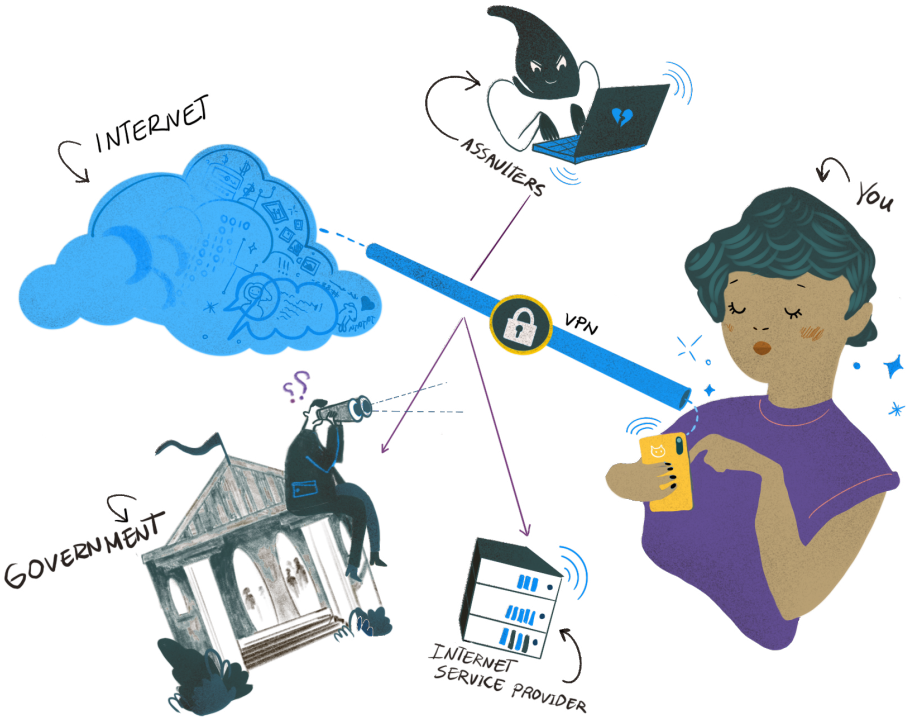
» *Content:*
Selene Yang – Nicaragua

» *Project supervision:*
Rosa Posa Guinea – Paraguay

» *Editing:*
Lucía Fernanda Bonilla – Guatemala

» *Translation:*
Ximena Soley – Costa Rica

With the support of



Feminist Digital Self-Care Manual