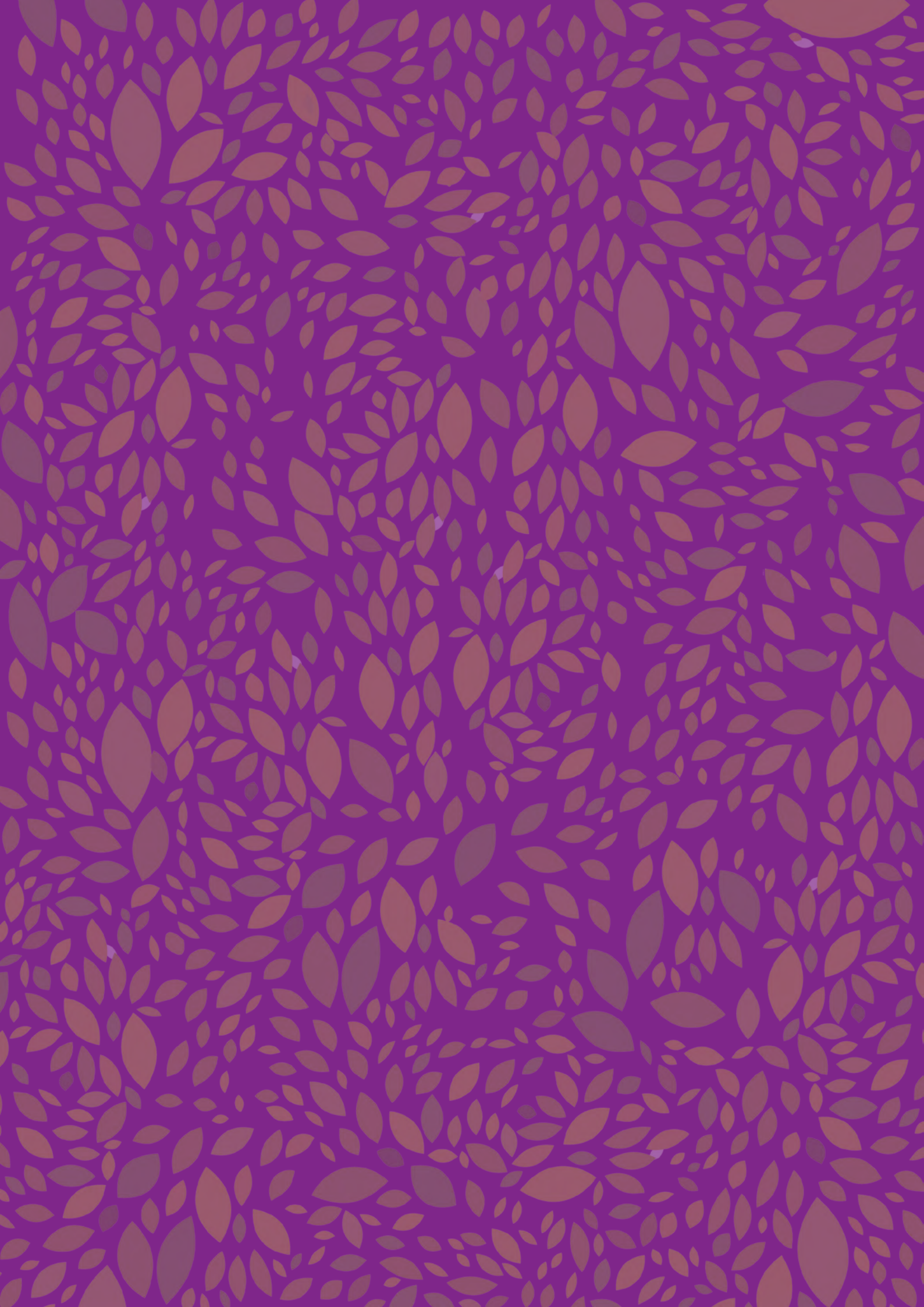


DIGITAL SECURITY AND FEMINIST HOLISTIC PROTECTION

AS PART OF TEMPORARY RELOCATION PROGRAMMES
FOR HUMAN RIGHTS DEFENDERS





DIGITAL SECURITY AND FEMINIST HOLISTIC PROTECTION

As part of temporary relocation programmes
for Human Rights Defenders



Created by:



Digital
Defenders
Partnership

Financed by:

calala

Fondo de Mujeres

In collaboration with:



Generalitat
de Catalunya



Agència Catalana
de Cooperació
al Desenvolupament

AUTHORS:

Alexandra Haché:

Project Officer, Rapid Response Networks and the Gender Equity and Diversity Inclusion strategy, Digital Defenders Partnership.

Ana Bermúdez Fong:

Regional Project Manager for Latin America

G

Project Officer for Latin America, Digital Defenders Partnership.

Mayelí Sánchez Martínez:

Digital security facilitator, Digital Defenders Partnership.

About Calala Fondo de Mujeres:

Calala Fondo de Mujeres is a foundation that promotes the rights, empowerment and leadership of women in Latin America, the Caribbean and Spain, through the deployment of resources aimed at strengthening women's and feminist organizations, networks and movements. Calala works for the consolidation of the feminist movement and focuses on strengthening grassroots women's and feminist groups which carry out work based on situated knowledge and intersectionality. At Calala, we seek to contribute to secure feminist activism, and this is why we are committed to developing the strategies and feminist holistic protection tools available to women defenders. <https://calala.org/>

calala

Fondo de Mujeres

www.calala.org

calala@calala.org

@FondoCalala

@calalafondodemujeres

@CalalaFondo

About the Digital Defenders

Partnership:

The mission of the Digital Defenders Partnership (DDP) is to provide a comprehensive response to digital threats and risks, to create resilient and sustainable support networks for people who defend human rights. To this end, DDP offers funds to respond to emergencies and provide sustainable protection. In addition, it contributes to strengthening rapid response networks and local protection, to improving the capacities of facilitators through grassroots work initiatives, and to long-term organizational security through the Digital Security Accompaniment Programme.

www.digitaldefenders.org/es/

We wish to thank all the defenders who agreed to be interviewed for this report for their time and generosity, as well as the following organizations for sharing their experiences during its creation and revision.

Contributors:

CEAR Euskadi, Comissió Catalana d'Ajuda al Refugiat, Defendred, Martin Roth Initiative, PBI Catalunya, Programa Barcelona Protege a Periodistas de México, Protect Defenders, Taula per Mexic.

Reviewers:

Victor Arias (DEFENRED - Red de Apoyo a Defensores y Defensoras de Derechos Humanos)

Marusia López
(IM Defensoras)

Daniel O Clunaigh
(Digital Defenders Partnership)

Maria San Martin
(Front Line Defenders)

Flo Pagano
(Digital Defenders Partnership)

CONTENTS

INTRODUCTION	8
A. INCLUDING DIGITAL SECURITY WITHIN TEMPORARY RELOCATION PROGRAMMES	11
B. RISKS IDENTIFIED IN THE RESEARCH	15
a) Applying to the programme	
b) Selection and communication between defenders and organizations for departure procedures	
c) Departure and border crossing	
d) Accommodation	
e) Relocation to the country hosting the TRP	
f) Planning for return	
g) Return trip and border crossing	
h) Communication once back at home	
C. RECOMMENDATIONS	36
a) Fostering a holistic approach to digital security	
b) Addressing Gender-Based Online Violence	
D. BIBLIOGRAPHY	43
E. ANNEX	45

INTRODUCTION

For more than 20 years, a number of programmes for the temporary relocation of defenders have operated in Spain. Temporary relocation programmes represent an option to improve the safety and well-being of Human Rights Defenders (HRDs) when other forms of protection have been exhausted at the community or national level.

Given the current socio-political context and the situations of violence and aggression that human rights defenders increasingly face, it is essential that the projects and programmes that work with Human Rights Defenders, and Women Human Rights Defenders (WHRDs) continue to promote and deepen practices for holistic protection and digital security.

This document is a translation and transposition into English of a report focused on temporary relocation programmes in Spain¹. It gathers elements that may be of particular interest for any temporary relocation programmes oriented at Human Rights Defenders, regardless of the geographical area in which they are located. As such, this document focuses primarily on presenting the challenges that exist for temporary relocation programmes in terms of the intersection that exists between Information and Communication Technologies (ICTs)², feminist holistic protection, and digital security. In addition, it presents a set of recommendations covering how to best include digital security and mitigate Gender-Based Violence Online within these programmes.

As part of this research, Feminist Holistic Protection provides the basis for a theoretical-practical framework that allows us to highlight the interconnection between psychosocial and emotional wellbeing, physical security and digital security, as well as individual and collective healing and recovery, as key elements in the sustainability of the defense of human rights.

1 Find the Spanish version of this document here: https://donestech.net/files/seguridad_digital_final.pdf

2 In the Spanish version we use Technologies for Relationships, Information and Communication since some initiatives oriented at digital inclusion and/or digital security in Spain have started to use the term technologies for relationships, information and communication (TRICs) in order to underline the crucial role of ICTs in creating and maintaining social networks and relationships. For this report we will use the term ICTs.

Feminist Holistic Protection is an approach proposed by Mesoamerican women defenders, particularly the Mesoamerican Initiative of Women Human Rights Defenders (IM-Defensoras)³. In their experience, Feminist Holistic Protection consists of:



A political and strategic framework in permanent collective construction. This approach provides an inclusive vision that allows us to put the care of our bodies, our organizations and our struggles at the center of political activism so that it remains viable in the face of constant violence and repression⁴



This approach is based on a feminist and collective ethos of care. This ethos is built from an intersectional feminist appreciation of context and risk that allows us to analyze how violence against HRDs, in its manifold forms, is committed, with the aim of perpetuating structures of oppression.

From this vision, networks of and for defenders are established, in which we take care of each other and take an active role in the protection process. These networks promote safe and trustworthy spaces in which to discuss the violence that affects us, and give Women Human Rights Defenders the power to construct their own responses.

Based on an enhanced risk assessment exercise, protection plans and processes are developed that join up a diverse range of strategies: emotional and therapeutic support, safe relocation, spaces of refuge and respite, healing processes, “political embodiment” understood as corporeal responses to injustice, safe communication and digital security, public protest, and protection of advocacy on a national and international level.

Feminist holistic protection is a response to the violence resulting from the patriarchal and capitalist systems and the work of defending human rights as it intersects with other structures of domination. It recognizes defenders as autonomous individuals, but also responds to their family needs and builds processes with their communities.

³ Read here more about it <https://im-defensoras.org/es/>




⁴ Read here more about it https://justassociates.org/sites/justassociates.org/files/programas_proteccion_defensoras_latinoamericadef.pdf

In addition to this definition of the different layers that make up Feminist Holistic Protection, we have also chosen to build and promote a broad and inclusive digital security outlook that focuses not only on securing information and communication channels, or on providing strategies and tools for confronting digital emergencies and/or Online Gender-Based Violence, but also on bringing together socio-political, psychosocial, collective and individual spheres in order to introduce measures and norms for collective support in digital environments. Constant changes in applications or devices drive us to consider social and practice changes instead of aiming only at the specific teaching of digital security tools. Technologies are the result of social dynamics and relationships that, in turn, arise from our use, appropriation and reappropriation of them.

This report is divided into two parts. The first part delves into the possible risks which can arise during the various stages of the temporary relocation process which were raised in the interviews and the literature review carried out. In the second part, we propose recommendations for mitigating risks during the temporary relocation process from a feminist holistic protection perspective, with a focus on digital security.

From a feminist protection point of view, we understand temporary relocation programmes as a sequential process, with particular support provision and protection measures that vary according to the socio-political context, the personal situation of the Human Right Defender and their organisation, and the stage in the relocation process.

We hope that this document will allow existing programmes, as well as the ecosystem of organizations and defenders directly or indirectly involved in temporary relocation programmes to:

-  Analyze their practices in terms of the issues raised in this report
-  Access ideas and resources, including examples of holistic feminist protection already part of existing programmes, activities and organizations
-  And participate in conversations and debates to continue improving international cooperation work for the protection of Human Rights Defenders

A

Including digital security within temporary relocation programmes

Digital security is increasingly considered of particular importance within temporary relocation processes. According to our research, both relocation programmes and local partners and defenders increasingly view digital security as essential in order to be able to carry out their work. In this regard, we have identified three different areas in terms of the incorporation of digital security within programmes:

Firstly, there is the standardization and search for “safe” tools for communication, documentation, and the correct management of sensitive and personal data and information by the organizations that coordinate the programmes. Nevertheless, there is a lack of implementation in certain parts of the spectrum of organizations that play a part in temporary relocation programmes (including partner associations⁵, ministries and embassies, airlines, welfare service providers and the press, among others).

Secondly, it is our consideration that there is a continuing need to develop and maintain protocols as part of the standardization of the use of secure tools for communication and information management. This relates to the security in office spaces, safe houses, (digital) spaces related to the programme, and spaces in which the various stakeholders involved in temporary relocation interact. Awareness-raising around the need to implement security measures can be further reinforced through the creation and maintenance of security protocols. It is this that makes it possible to transform the need for security into a new organizational culture.

Finally, the content and training aimed at relocated defenders concerning these issues remains piecemeal and is subject to differing approaches across existing programmes.

⁵ By partner associations, we mean defenders’ organizations located in their country of origin, as well as those organizations located in the country hosting the TRP that act as a conduit between the defender and the temporary relocation programme.

Even though there is openness and willingness to change in order to create and uphold new digital security practices and protocols, we have detected a certain degree of pessimism, as expressed in the following quote from an interview with a programme coordinator:

“ *Even though we might do so, the implementation of good practices or safe tools can't be guaranteed across the board* ”

This reflection highlights the intertwined nature of information and communication technologies, in which there are always several people with access to and oversight of the same data, each of whom could prove, consequently, to be a possible weak link in the security chain. Data-oriented security and ICTs require individual and collective actions and responsibilities, even more so in an environment as complex and diverse as that which envelops temporary relocation programmes. Recognising that digital security is everyone's responsibility can easily become a discourse that transforms this need into an unattainable goal. Moreover, we have also seen digital security considered as an unattainable goal because it requires technical knowledge that, ostensibly, only experts such as programmers or computer scientists would possess. Although it is true that our capitalist and consumerist societies promote unbridled and thoughtless consumption of ICTs, and a lack of interest in fostering spaces for citizens' education and social use of these technologies, we believe it is important that temporary relocation organizations and programmes avoid promoting discourses that sanctify digital security as a matter for experts only. Both perspectives give rise to disempowering and paternalistic discourses that dissociate programmes, stakeholders and defenders - with their own daily experience and expertise - from technologies for relationships, information, communication, documentation and memory creation.

In terms of temporary relocation programmes, our interview with Protect Defenders⁶ and EU-TRP⁷ highlighted that many programmes are also beginning to incorporate digital security tools and protocols in the three areas that we have indicated. Some of these programmes are engaged in a process of reflection on digital security following the shifting of many face-to-face activities to digital spaces as a result of the COVID-19 crisis. This forced and

6 <https://protectdefenders.eu/>
7 <https://eutrp.eu/>

urgent migration towards digital spaces has also made it possible to identify the limits and risks inherent to these channels and platforms, forcing an across-the-board rethink of digital security strategies more clearly.

We have also identified temporary relocation programmes that incorporate digital security in several of these areas, and that can serve as reference points and/or examples of good practice for other programmes interested in exploring these issues. Here, we include the following programmes: Martin Roth Initiative⁸ , Elisabeth Selbert Initiative⁹ , Reporters Without Borders¹⁰ in Germany, Shelter City¹¹ in the Netherlands and the European Center for Press and Media Freedom¹² at the European Union level.

It is important to stress that several of these programmes are aimed at journalists and cultural stakeholders. This further demonstrates the need to offer training content on digital security especially designed for these profiles of HRD as they are considered as particularly exposed to digital attacks, as well as specially with the need to know how to protect their sources, documentation and communication channels.

Although it is important to give special priority to providing content and training on digital security for defenders professionally involved in defending and raising awareness regarding freedom of expression, information and communication (journalists, bloggers, developers, data analysts, authors, artists etc.), we also wish to emphasize that all HRD depend on, to a greater or lesser extent, and interact with technologies for relationships, information, communication, documentation and memory creation. Therefore, we believe it is important to broaden the focus on digital security to include the promotion and incorporation of activities and training that allow HRD and local organizations to receive training in the political, tactical, and creative uses of ICTs. This approach should always incorporate a feminist perspective of technologies that questions their impact on fundamental freedoms in relation to security, privacy and sustainability.

It is also necessary to break with the view that the security of ICTs is a matter for computer experts, and take into account the fact that - given the reach of such

8 <https://www.martin-roth-initiative.de/en>

9 <https://www.ifa.de/en/fundings/elisabeth-selbert-initiative/>

10 <https://rsf.org/en/germany>

11 <https://justiceandpeace.nl/en/shelter-city-paises-bajos-convocatoria-para-reubicacion-temporal-en-2021/>

12 <https://www.ecpmf.eu/>

technology - we are all obliged to interact with it, in terms of socializing, sharing ideas and offering bottom-up popular education about these technologies and what they mean in our everyday lives and in the lives of defenders.

We also believe that it is important to value the experience of HRD, and specially WHRD regarding ICTs and digital spaces, insofar as we are all experts in our own relationships with those technologies and how we inhabit those spaces. Therefore, the construction and maintenance of safe and comfortable spaces on the internet must be considered a necessity, in order to protect and strengthen digital and human rights, and temporary relocation programmes must find ways to contribute to this collective effort.

This assessment is a synthesis of the main aspects detected in the development of feminist holistic protection, care and digital security as part of the TRP interviewed in Spain and, to a lesser extent, in the EU. As such, it is an incomplete snapshot of the current landscape, and one which will need to be retaken on a regular basis in order to keep track of developments and changes occurring in the field of temporary relocation programmes. Further this assessment, we now break down the risks for HRD and their organisations related to TRP that have been identified in the course of our research, followed in the last section by a series of recommendations for dealing with, mitigating and/or overcoming some of these risks.

B

Risks identified in the research

The complexity of the process of relocating a defender is apparent when we consider the risks at the different stages of the process. The interviews and literature review carried out show that there is a large amount of accumulated knowledge about risks and how to mitigate them, but also a sense that other aspects still need to be addressed, as well as the need for a paradigm shift and a wider selection of tools for undertaking increasingly holistic protection work.

Based on what was shared with us in the interviews, and from our own experiences, we have undertaken an analysis of the risks detected, prioritizing those to which insufficient consideration is given in relocation programmes, and which are less easily conceived of. We have chosen to classify these risks within the broad categories of risks to psycho-emotional security, risks to physical security, risks to digital security and, in some cases, also risks to economic security, although we understand that many of these are overlapping. We also wish to stress that these risks, except in some very specific moments of the process, can be very different depending on the conditions of the defenders. It is important to recognize that each temporary relocation programme has its own idiosyncracies and approaches and, as such, the risks that emerge should be seen in context rather than in a vacuum.

By approaching relocation processes from a sequential perspective, the following risks for WHRDs and for organizations managing temporary relocation programmes can be seen.



A) APPLYING TO THE PROGRAMME

RISKS TO PSYCHO-EMOTIONAL SAFETY

Uncertainty regarding financial dependents:

When applying to a programme, the defender must make decisions regarding whether or not to bring their financial dependents with them, or how to guarantee their sustainability and well-being during relocation. Not all programmes offer this type of support, and it is possible that defenders will decide not to apply if they do not receive adequate assurances in such cases.

One-sidedness in the establishment of trust between the programme and the defender:

Establishing trust is almost always a question for those who manage the relocation programmes or who accompany the application to the programme regarding the defender. This is particularly notable in the relative fluidity of processes in which those who provide references about the work of the defender are on the radar of the organization that runs the relocation programme.

However, trust in the other direction - that which the defender places in the programme and in the people who will be points of contact during the application process - may not be afforded the same weight. Furthermore, during the application process defenders provides information that place them in a vulnerable position, insofar as such information would elicit a positive response to their application. Risks arise when this relationship of trust is not established bilaterally, resulting in the defender not communicating certain data, feeling demeaned by the application process, or the process taking longer on account of defenders' misgivings.

Appropriation of the application process:

Sometimes defenders have difficulties in submitting applications on their own, either due to their own personal capacity and resources, the complexity of application forms, and so on. As a consequence, they resort to the help of allied persons or organizations in order to complete their application. This may entail different types of risk, for example, that the defender loses control over the information submitted as part of their application, as well as in how it is presented. There may be a lack of communication and understanding about the process within the organization or community to which the defender belongs, giving rise to fissures in these organizations or communities. In some cases, an entire community is involved, and there is a risk of bias in internal decision-making processes regarding who should apply for relocation, and under what circumstances.

RISKS TO DIGITAL SECURITY

Applications and communication channels without adequate protection of sensitive information:

Where there is the possibility of sending the application by e-mail, if both the defender and the programme do not use e-mails that implement encryption by default, there is a risk of exposing sensitive information. In the event that cloud platforms are used to upload files or web forms, it is important to verify the access and secure storage conditions of these platforms, as well as to have clarity on applicable legislation with regard to possible requests for information by government entities.

Loss of information or access to information channels:

in the process of applying to a relocation programme, there are several stages at which urgency and uncertainty can affect the defender's psycho-emotional well-being, rendering some steps more complex than would otherwise be the case. Should a defender need to create a more secure e-mail account to maintain communication, there is a greater risk that they will forget passwords or lose access to that means of communication, either due to theft, seizure or loss of the device, leaving them without a secure channel of communication.

Lack of means or resources to guarantee secure communication:

The circumstances in which defenders apply to these programmes are so varied that access to secure communication cannot always be guaranteed. For example, it may be that the defender cannot install a secure communication application on their device if they do not have the technical capabilities to do so, their device does not support the application, they do not have access to an internet service or readily available electricity, or they cannot afford to pay for mobile data, among other reasons.

B) SELECTION AND COMMUNICATION BETWEEN DEFENDERS AND ORGANIZATIONS FOR DEPARTURE PROCEDURES

RISKS TO PSYCHO-EMOTIONAL SAFETY

Discrimination by authorities and embassies:

There is a risk of discrimination against defenders in departure procedures, for example, on grounds of racialization or because of other aspects such as their economic situation. Defenders sometimes do not have passports and must go to local authorities to get one, exposing them to risk insofar as national immigration authorities may deny the issuance of travel document, resulting in the defender having to rethink their exit strategy.

Bureaucracy and time to complete the procedures:

Procedures for obtaining visas, passports and other documents necessary for the trip are usually cumbersome and bureaucratic. In addition to the risk of discrimination mentioned in the previous paragraph, service and response times also place an emotional burden on defenders. For example, in the experience of one of the people interviewed, holiday periods in Europe significantly held up procedures. As a result of COVID, the use of documented exceptions to cross borders, such as the certification of official invitations by the embassy, has increased bureaucracy. For some defenders, relocation to another country may represent their first time abroad, meaning that it is likely that they would never have completed the passport process, and may not even have the resources to do so.

Lack of resources for relocation and related procedures:

Some programmes offer financial support to defenders in this regard. However, this is usually offered as reimbursement for expenses incurred. Defenders may not have sufficient resources to be able to take on the costs of relocation and related procedures. They may be human rights defenders who live in remote and inaccessible areas, increasing the cost of the move and - considering that most of these procedures are not immediate - entailing additional lodging, food and transportation costs in the meantime.

PHYSICAL SECURITY RISKS

Internal relocation in high-risk areas:

In cases where defenders need to move to a different city to carry out departure procedures (application for a passport or visa), there are additional related risks. These risks may arise from having to travel through highly dangerous areas, going through checkpoints (be they police, paramilitary, non-governmental armed forces, etc.), using unsafe or unreliable transport, as well as from ignorance of crime rates in the city to which or the area through which they travel to carry out departure procedures.

RISKS TO DIGITAL SECURITY

Loss, seizure or theft of equipment:

In the process of completing procedures for departure, defenders must interact with one or more official bodies. During this part of the relocation process, the risk of loss, theft and seizure of equipment is greater, since defenders find themselves, on many occasions, in unfamiliar environments and government buildings where their personal effects may be searched. It is also important to remember that defenders will be traveling through spaces where crime rates may be high, representing a risk of theft and loss of equipment and information.

Use of communication tools without considering information security and privacy:

In addition to the risks mentioned above, the use of tools or applications for communication that do not adequately take into consideration the privacy and security of information may negatively affect departure procedures. Certain tools are not sufficiently secure and do not store information properly, entailing a risk of information theft and seizure of equipment by local authorities.

Information management by state institutions:

At this stage, interaction with government agencies is frequently necessary in order to complete procedures. It is possible that due care of information may be compromised if such agencies do not have adequate security mechanisms in place for the sending and receiving of information.

C) DEPARTURE AND BORDER CROSSING

PHYSICAL SECURITY RISKS

Depending on the particular circumstances of each defender, their departure can be extremely high-risk.

Arbitrary arrest and detention:

When defenders depart and cross borders via migration centers, they run a high risk of being arrested or detained upon being identified for their work. Some defenders face political criminalization for the work they do, and some are subject to court orders that can make it difficult for them to move freely across borders. Although detention can sometimes be temporary, it may entail missing transport connections and having to incur extra expenses. Defenders may be detained at the border, supposing a greater risk to them inasmuch as certain aspects of their safety and well-being cannot be guaranteed. These risks are higher for trans individuals, especially if their appearance differs from the gender included in their identity documents.

Being victims of common crime:

During the trip, defenders may fall victim to crime which is not necessarily targeted at them, but which is part of the everyday reality of the area through which they are traveling on the way to their destination. It may be the case that their chosen transport crosses high-risk areas particularly affected by crime, the presence of criminal organizations, etc.

Use of non-official border crossings to leave the country:

In some cases, defenders cannot cross borders legally, entailing the use of other means to leave the country and protect their life. Many defenders are forced to use so-called “blind spots” or little-traversed routes where the risk of suffering serious physical harm increases.

Lack of knowledge of whereabouts:

For some defenders, knowledge of their departure can signify a high risk to their community and, as such, they are obliged not to notify their relatives, leave at dawn, use little-traversed routes, etc. If a communication strategy has not been developed regarding certain aspects of the trip, including how to manage departure with family members and the community, there is a latent risk of unnecessary alerts being raised.

Arrests or detentions in the destination country:

If the defender is not clear about what to do, what to say, or even what documents to show when arriving in the destination country, it is possible that border officials will detain them. It is important to remember that, when defenders in situations of risk leave their country of origin, their emotional state sometimes makes it difficult for them to respond with certainty to the questions they may be asked upon arrival at their destination.

RISKS TO DIGITAL SECURITY

Lack of security protocols:

If a security protocol is not established which takes into account various aspects such as communication during the trip, what to do with sensitive information, what information to protect and what information to travel with, defenders may be placed in a position of vulnerability entailing a range of risks, including those mentioned above, in terms of their physical and psycho-emotional safety.

Unintentional disclosure of location by means of device used:

The defender may reveal their location during travel due to the use of cell phones, either as a result of having the GPS active, of sharing information on digital social networks, or of cell triangulation provided by service providers.

Profiling through social networks:

Both when completing visa procedures and when crossing borders, public officials may request disclosure of the profiles of the defender's social networks. Although we consider this to be a violation of privacy, some governments request this information for official procedures and to "verify" the work of the defenders or allow passage across their borders. If the defender does not have a plan for the management of social networks during this period, they run the risk of criminalization for any publication or content that authorities consider an attack against the sovereignty of the country, even if such content relates to human rights campaigning.

Communication on social networks:

This risk is related to the aforementioned and includes the possibility that the defender communicates their departure from the country to other parties via insecure networks. Likewise, communication with family members, although important, also poses a risk if it is not carried out securely, and if specifically-defined periods in which communication is possible are not established.

Loss of information or lack of backups:

At the border crossing, it is possible that the defender will be asked to provide access to their devices and, if they do not have a protected backup (remote or otherwise), the information contained on these devices may be exposed to people that should not have access to it. Another related risk is that the device is stolen during transit.

Recovery of deleted information:

In the event that devices are requisitioned at the border crossing, if the defender has not carried out a secure deletion of sensitive information, public officials with technical knowledge could seek to recovery information stored on their device, potentially exposing information that was previously considered deleted.

D) ACCOMMODATION

RISKS TO PSYCHO-EMOTIONAL SAFETY

Depending on the programme, accommodation may be private or shared, which can bring with it various risks such as:

Depression due to isolation: the defender will find themselves in a space that they know is temporary and in a different environment from that which they are used to, in some cases sharing a house with unknown people who have other ways of living. All these aspects impact the psycho-emotional health of the defender. Even where a move with dependents is possible, the feeling of loneliness and hopelessness upon arrival may be high, without disregarding the relief of escaping from a dangerous situation. These contradictory feelings coexist within the defender insofar as they know that their stay is temporary.

Gender-based violence:

In programmes which welcome HRDs who defend different causes, it is possible that a given defender, although defending certain rights, has not deconstructed sexist or colonial attitudes and behaviors which, in one way or another, may negatively affect others participating in the programme. Such situations may likewise involve those who are part of the reception team.

Conflicts with cohabitants due to customs or prejudices:

Living in a house with defenders from other places and with other customs can also be an emotional burden. Attention-to-detail in the house, the cleaning or eating habits of other people, the sharing of food and schedules to undertaken certain tasks: all of this can create conflicts between people. Defenders who have different belief systems or who have suffered persecution and threats from governments with political affiliations opposed to their own also sometimes find themselves living together in the same space. As such, a figure who for one defender is destructive may, for another defender from another country, be an ally. This can cause conflict when sharing outlooks and experiences. It is important to be aware of the possibility that the defender may experience mistreatment, racism, discrimination or harassment by any of the people who participate in the relocation programmes or by their peers (other defenders).

RISKS TO DIGITAL SECURITY

Disclosure of accommodation location:

Some accommodation is deliberately undisclosed, so there is a high risk that the location is revealed by the use of cell phones or by connecting to internet services without using tools to hide it.

We appreciate that relocation programmes handle the disclosure of the location of the house or temporary residence in different ways, often under the assumption that the territories of the Global North are safer for defenders. However, it is important to note that the political interests of human rights defenders often exist in confrontation with those of international corporations and that, although circumstantially more or less probable given the country in question, an underlying risk always exists.

Interception of communications:

If trusted individuals who can provide a technical response to configuration needs problem-solving with the internet connection, routers, etc. are not available on-site, the risk of encountering poorly configured devices or attacks with the aim of intercepting communication is greater.

E) RELOCATION TO THE COUNTRY HOSTING THE TRP

RISKS TO PSYCHO-EMOTIONAL SAFETY

Lack of an adequate contextualization of the space:

This refers to how the cultural and legal situation of each defender are understood. It also covers problems in fitting in and properly appreciating the risks related to being in a different city or locality, and in a country with a different legal system. For example, false perceptions of the level of risk and failure to identify risks such as theft or gender-based violence may arise. Even changes in diet can be an influencing factor, in terms of fully understanding what products are available, and how to use them to maintain a balanced diet.

Dealing with public perception during relocation:

For some HRD, public perception of temporary relocation can raise risks for their return to their own community. Depending on the circumstances of the defender and their organization, certain perceptions can be especially harmful. The individualization or heroic treatment by the public of the defender can create additional tensions within organizations. The time spent away from their place of origin can weaken the political clout of the defender.

Psycho-emotional deterioration during relocation:

Even when the programme includes psychological support, there is a significant risk of psycho-emotional deterioration. This is especially important if the defender is used to living with more people and during relocation lives alone, or if the way in which emotions are processed in their culture is subject to other types of care, such as ceremonies with herbs or baths, use of infusions or teas, or if the management of emotions is collective, etc.

PHYSICAL SECURITY RISKS

Differences in risk management within the programme:

Lack of adaptation to how risks are managed during the programme can affect the defender. If the defender is used to collectively managing risk and is in a programme that affords greater individual responsibility, they may find this process overwhelming. In other cases, it is possible that the defender will carry out highly individual risk management and attempt to reach consensus with the relocation programme regarding security protocols.

RISKS TO ECONOMIC SECURITY

Familial economic instability arising from the departure of the defender:

The testimonies provided during the research point to the need to “tighten belts”, in order to save some of the money provided during the relocation of the defender and send it to their family. In many cases, the defender has indirect dependents who are also affected by no longer receiving the financial support that the defender provided them with. In other cases, the defender may decide to save part of the resources provided by the programme in case they are relocated again upon return, or if they are considering more permanent residency options should their situation not allow for planning for a return to their place of origin.

Possible loss of employment:

There are circumstances in which the defender cannot continue to carry out their professional work while in the relocation programme, either because of the specificity of their role or the conditions under which they are employed, which preclude working from distance.

RISKS TO DIGITAL SECURITY

Use of unsafe means of communication:

one of the most common risks factors while the defender is in temporary accommodation is communication with relatives, colleagues and friends at home. Although the programme may establish safe means of communication between those who are part of it, this does not usually extend to others in the defender's place of origin, or others with whom the defender maintains contact. If there is no awareness of the importance of safe communication with family and others, information that is sensitive to both the defender and other programme participants may be disclosed.

Revealing accommodation location:

This risk is mentioned above, and is a factor from the moment of arrival and through the duration of the relocation. Location can be unconsciously revealed by the use of GPS, home delivery applications, and uploading photographs to social media platforms with parts of the accommodation in the background or parts of the street where it is located. Some programmes do not allow third-party visits. Nevertheless, the defender may share their location with others in the country in which they have been relocated. In many cases, these are defenders who reside in the same city. However, this entails a significantly high risk, given the lack of knowledge concerning the security situation of these individuals.

E) PLANNING FOR RETURN

PSYCHO-EMOTIONAL RISKS

Uncertainty about return:

Planning a return after several months of being away from their community, organizations and political environment can generate stress and anxiety in defenders who do not know what they might face when they return. Likewise, planning a return involves reviewing possible risks and creating protection protocols that can increase feelings of uncertainty, fear and anxiety.

PHYSICAL SECURITY RISKS

Incomplete return plan:

It is difficult to address all the possible risks that the defender may face when preparing for return. However, the most significant risk arises from a lack of planning based on an updated risk analysis, including logistical planning for return and specific details including, but not limited to: arrival and contact times; parties who accompany the defender upon departure and arrival; follow-up on travel; emergency contacts in the place of origin and in the programme; the possibility of further temporary relocation within the country when they have returned, to allow the defender to adapt again; what happens if they are detained when crossing the border, and what actions to undertake in such circumstances

RISKS TO DIGITAL SECURITY

Request for digital security training at the end of relocation:

It is common that, when the time to return comes around, defenders request training in digital security. However, digital security training must be scaled, so that the defenders can identify what they need to learn and how to implement it, be trained in the new practices and tools they need, and in general have sufficient time to take onboard this new knowledge and translate it into good practice.

Not considering a digital security plan within the return plan:

even if there is a return plan, if it does not include measures to protect digital information and communications, in addition to management of electronic identities and profiles on social networks, there is an increased risk of exposing information about the defender and their movements and work, and information concerning the programme and other people who have participated in it.

G) RETURN TRIP AND BORDER CROSSING

PHYSICAL SECURITY RISKS

Arrest or detention at border posts:

Just as when leaving the country, this same risk is present upon return, and may be higher if there has been an increase in the defender's profile during their relocation. Likewise, knowledge of the defender's return may lead to their detention when crossing the border.

Monitoring and surveillance:

If the defender crosses the border and enters the country, or if the defender returns directly to their home and to their activism, there is a risk that they will be watched and followed by their adversaries.

Difficulty adapting upon return and location-specific risks:

In addition to the risks during departure, there is also the possibility that movement between areas of different risk categories becomes difficult for the defender. For example, upon being relocated, the defender may adapt to living in a location with less crime. When the time comes to return, the defender may not immediately regain the strategies they previously called upon to deal with this type of risk, or may become hyper-reactive, leading to notably higher levels of stress.

RISKS TO DIGITAL SECURITY

Loss, confiscation or theft of equipment:

When crossing the border and returning to their place of origin, border authorities may confiscate defenders' equipment or request access to information in their possession. Another possible risk is theft of devices, either by common criminals or as part of a targeted attack.

H) COMMUNICATION ONCE BACK AT HOME

RISKS TO PSYCHO-EMOTIONAL SAFETY

Breakdown in communication between the defender and the programme:

This occurs when there is no closure and monitoring plan once the defender returns to their place of origin, nor any care mechanism through which to report cases of abuse, discrimination or harassment experienced during relocation and/or return.

RISKS TO DIGITAL SECURITY

Failure to implement acquired digital security measures:

One of the digital risks upon return is that the defender stops using communication tools that improve information security and privacy conditions. In some cases, women defenders return to practices that can put their communications at risk, and this is sometimes due to the convenience of communicating with more people through insecure applications.

Recommendations

In this section we present specific recommendations aimed at creating a broad and inclusive approach to digital security, and how to better address Gender-Based Online Violence. In the following section, we also include a collection of resources that will help different stakeholders to use these recommendations as a springboard for implementing new practices that protect defenders, local partner organizations and temporary relocation programmes.

The experience that Latin American WHRDs and Civil Society Organizations have in terms of the feminist holistic protection model provides a frame of reference for these recommendations and a focus on physical, psycho-emotional and digital security protection.

We ask that these recommendations be considered in relation to the experience and approach of each temporary relocation programmes.

I. Fostering a holistic approach to digital security

The legacy of colonialism in technology is the continuity of capabilities and practices that are tied to racism, discrimination, and the rejection of sexual and gender diversity. It is under these precepts that preconceptions arise about who makes technology and who can use it. Technology is not neutral, and it is no coincidence that many of us believe that only experts (programmers or computer scientists who often happen to be also men) can implement digital security on a daily basis.

This assumption is the result of a colonial, patriarchal and capitalist perspective regarding technology and the digital realm. Appropriating technologies politically, tactically and creatively is therefore also a matter of decolonization and de-patriarchalization. It is a question affording space and recognition to the knowledge acquired by our ties with and daily use of ICTs.

We use ICTs and spend time in digital spaces every day. All of us are experts in our own relationship with these technologies. When we use and configure our mobile phones, when we decide where we store our information (on a pen drive or in the cloud), when we make backups or delete data, when we use social media platforms for certain purposes, when we decide whether to upload photos of ourselves or of our children, or what e-mail we use for our communications, we are making everyday decisions about what these technologies represent. As a result, it is important to take the time to reflect on the uses and decisions we make with technology, given that, in this reflection regarding what we do and why we do it, we may broaden our appreciation of digital privacy and security. To this end, our recommendations are the following:

DEMYSTIFY AND POLITICIZE ICTS:

- Demystify and politicize ICTs, stop treating them as areas limited to information technology experts, and organize collective reappropriations of these technologies through popular education processes.
- Recognize the capabilities, knowledge and strategies of HRDs, and especially WHRDs, regarding their own uses of and experiences with ICTs.
- Stop seeing digital security as something unattainable. While it may be true that digital risks can occur throughout the entire chain of interconnected spaces, no one can ensure all the dimensions connecting ICTs (identity and memory management, handling of personal and sensitive information, geolocation, and management of contacts and relationships). Nevertheless, this should not lead to a sense of despondency and powerlessness. Digital security is a journey that is undertaken with patience and in which all actions count. It's better to put small digital security steps in place than to not implement any at all.
- Take responsibility for the full range of our uses of and relationships with ICTs. Choosing certain ICTs, spaces and digital platforms over others brings consequences for the defenders with whom we interact. These consequences can range from causing anxiety as a result of not knowing how to use such technology, to putting defenders at risk through a lack of high safety standards.

- The basics of digital security such as updating operating systems, use of antivirus and firewalls, secure connection to the internet through VPNs, use and management of secure passwords, as well as privacy and security configuration of accounts on platforms, represent the most significant steps towards ensuring good levels of digital security. It is essential to start normalizing these dimensions across the entire sphere of temporary relocation programmes.
- Secure internal and external communication channels, as well as the management of defenders' identifiable and sensitive personal data, and the documentation of the programmes themselves, are of the utmost importance. Implementing data archiving, erasure and retention policies in temporary location programmes remains outstanding.

EXPAND THE FOCUS OF DIGITAL SECURITY AND DEVELOP ADAPTED CURRICULA FOR TRAINING:

- Expand the focus of digital security from a feminist self-defense perspective in terms of physical security (toolkit training), self-care (taking care of our data and the data that we keep on other people), healing (devices that harm us and our planet), collective and historical memory (data preservation and policy), and obtaining justice (restorative and transformative processes).
- The training provided to HRDs concerning ICTs must involve a feminist perspective that questions the impact of technology on fundamental freedoms, security, privacy and everyday sustainability. In addition, it must take into account defenders' experiences, journeys and goals, and proposed curricula and training methodologies must be adapted to their circumstances, see for example: Cyberherbology and Ancestral Medicines and digital security (Vita Activa and NVA) or Convite (Nois Radio)
- The training provided concerning ICTs and digital spaces should encourage a critical, political, tactical and creative approach to these technologies among HRDs, focused on their needs as defenders. Training content should not be limited to the securitization of communication channels used by defenders, but should also include other areas that could be of interest to them, for example: detecting

and preventing Gender-Based Online Violence, documenting human and environmental rights violations, sharing or sending information via the internet as anonymously as possible, creating efficient online awareness campaigns, using multimedia tools for audiovisual production (gifs, memes, videos, audios), protecting web pages from attacks and censorship, developing more sustainable uses of ICTs, managing electronic identities and online credibility, physical safety and asset security, detecting and counteracting surveillance mechanisms, practice with free cartographic tools, use of tools to monitor environmental contamination, digital literacy, and creation of safeguards and secure digital files, among others possible topics. We recommend not offering digital security training to defenders who do not have prior user experience of technologies or devices such as cell phones or computers, since counterproductive situations may arise in which the defender could feel excluded and discriminated against. Offer technological literacy training for defenders who require it so that they can learn the basic concepts of computer science and internet use.

- First, assess if HRD require practical training regarding specific tools, or if it is better to work on raising awareness about the challenges ICTs entail for fundamental freedoms such as security, privacy and everyday sustainability. These activities should be aimed at making it easier for defenders to later discuss these issues within their organizations and communities.

MAKE GLOBAL AND LOCAL NETWORKS VISIBLE AS PART OF A HOLISTIC DIGITAL SECURITY MENTORING:

- Strengthen alliances with organizations, groups and local activists working for feminist holistic protection and digital security, in order to offer safer and more welcoming temporary relocation application processes for defenders. These mentorships should be considered when applications are made to the programme, upon departure from applicants' place of origin, and upon return.
- Make it easier for HRDs to learn about digital rights organizations and funds that support defenders who face digital risks or emergencies. Inform them about the organizations which they can apply to in order to receive support, advice or resources to migrate to safer

infrastructures and/or undertake risk analysis, as well as training and mentoring adapted to the needs of their organizations and communities.

- Find out about organizations, groups, or local networks that could advise and support defenders on digital security issues once they return home.

MAINTAIN SHARED TECHNICAL AND RESOURCE INFRASTRUCTURE:

- Encourage the creation of shared resources between different relocation programmes. These could consist of lists of groups that offer training to defenders in different areas, repositories of guides and digital security tools, as well as security protocols for each of the programmes.
- Endeavor to share the costs of installing and maintaining secure infrastructure and tools for programmes and defenders (Jitsi, Big Blue Button, Nextcloud, Jirafeau, encrypted emails, etc.). This could include having secure facilities for videoconferences, webinars, documentation, safeguarding of important documents for defenders while they travel, shared agendas and calendars, etc.

II. ADDRESSING GENDER-BASED ONLINE VIOLENCE

Gender-Based Online Violence includes threats, defamation, hate speech, racism, harassment, extortion or identity theft. Although these incidents may not be considered serious insofar as they lack a purely physical manifestation, such forms of violence are ever-present on digital platforms and networks used by Women Human Rights Defenders. Furthermore, online attacks against women and LGBTQI+ defenders are strategically targeted to discredit and/or undermine their political participation.

Because attacks against women defenders are normalized in public spaces, both offline and online, and are also often sexualised, too often little importance is given to the effects they have on our bodies, psyches and emotions. Florencia Goldsman reminds us that “All these forms of aggression affect the lives of women, because they result, among other things, in reputational damage, isolation, alienation, limitations on movement, depression, fear, anxiety and sleep disorders” (2020). For this reason, it is increasingly important to bring this type of violence to people’s attention and to stop normalizing it. We must visibilize the forms it takes, its effects and, above all, come together under the banner of digital feminist self-defence so that our voices continue to be heard loud and clear in digital public spaces.

Gender-Based Violence Online (GBVO) violates the fundamental rights of freedom of expression, privacy and the right to a life without violence. As such, it is important that they are picked up on within the temporary relocation programmes during risk analysis, in protection plans and in collective and/or individual therapeutic processes.

In order to better include the identification and mitigation of GBVO into TRP recommend the following:

- ▶ Develop protocols to address gender-based violence against women and LGTBQI+ people and train programme workers, partner associations and defenders so that they know how to use them and how to report gender-based violence.
- ▶ Address gender-based violence and GBVO in risk and protection protocols as key issues during defenders’ relocations, both outside of and within their country or area of origin.

- ▶ Include training that addresses GBOV, the ways in which such violence is manifested, and strategies to deal with it. Offer training focused on managing women defenders' electronic identities and digital spaces as part of a feminist self-defense perspective.
- ▶ Address GBVO as part of wider healing or psychosocial processes.
- ▶ Those who coordinate programmes should be trained in how to detect and provide support to defenders who experience GBVO.
- ▶ Facilitate access to resources and platforms which provide information about GBOV, and which highlight the broad range of cyberfeminist collectives or organizations that provide support on such issues in Latin America and around the world.

Bibliography

Asociación por la paz y los Derechos Humanos Taula per Mèxic. 2020. Yo sí te conozco. Las voces que acompañan: Taula per Mèxic.

Recuperado de:

https://www.taulapermexic.org/wp-content/uploads/2020/12/INFORME_YOSITECONOZCO-digital.pdf

Bartley, P. 2020. Wellbeing During Temporary International Relocation: Case Studies and Good Practices for the Implementation of the 2019 Barcelona Guidelines. Stuttgart: ifa (Institut für Auslandsbeziehungen).

Recuperado de:

<https://doi.org/10.17901/akbp1.14.2020>

CAHR, ICORN, Justice and Peace Netherlands, The Martin Roth Initiative, Adam Brown of The New School in New York, and Sasha Koulaeva. 2010. Las Guías de Barcelona sobre el bienestar y reubicación temporal de las personas defensoras de Derechos Humanos en riesgo.

Recuperado de:

<https://static1.squarespace.com/static/58a1a2bb9f745664e6b41612/t/5e17d777f4f2d729347ba666/1578620792321/The+Barcelona+Guidelines+-+ES+%28Final%29.pdf>

Cuny, L. 2021. Reubicación de Artistas en Riesgo en América Latina. (ifa-Edition Kultur und Außenpolitik). Stuttgart: ifa (Institut für Auslandsbeziehungen).

Recuperado de:

<https://doi.org/10.17901/AKBP1.07.2021>

Goldsman, Florencia. 2020. Preocuparse y ocuparse. Cuidados digitales ante un internet cada vez más violento. En www.pikaramagazine.com.

Recuperado de:

<https://www.pikaramagazine.com/2020/07/precuparse-y-ocuparse-cuidados-digitales-ante-un-internet-cada-vez-mas-violento/>

López, Marusia. 2018. La protección a defensores y defensoras de derechos humanos en Latinoamérica desde una mirada feminista. Retos y perspectivas de los programas de reubicación temporal y otras iniciativas de protección en el Estado Español: Asociadas por lo Justo.

Recuperado en:

https://justassociates.org/sites/justassociates.org/files/programas_proteccion_defensoras_latinoamericadef.pdf

López, Marusia. 2018. Desafíos y propuestas para el fortalecimiento de los programas de reubicación temporal para personas defensoras. Una mirada feminista desde la experiencia del estado español.

Recuperado de:

<https://www.justassociates.org/es/publicaciones/desafios-propuestas-fortalecimiento-programas-reubicacion-temporal-personas-defensoras.pdf>

IM-Defensoras. 2020. Protección integral feminista para transformar la crisis en tiempos de COVID-10: Iniciativa Mesoamericana de Mujeres Defensoras de Derechos Humanos.

Recuperado en:

<https://im-defensoras.org/wp-content/uploads/2020/11/IMD-16Dias-Esp-Final.pdf>

Michaelsen, Marcus. s.f. Silenciamiento a través de las fronteras. Represión transnacional y amenazas digitales contra activistas exiliados de Egipto, Siria e Irán: Hivos.

Recuperado en:

<https://hivos.org/assets/2020/02/SILENCING-ACROSS-BORDERS-Marcus-Michaelsen-Hivos-Report.pdf> [En inglés]

Peace Direct. 2021. Descolonización de la ayuda y consolidación de la paz. En www.peacedirect.org.

Recuperado de:

https://www.peacedirect.org/timetodecoloniseaid_es/

Schagen, N. v. 2020. Collaboration Between Temporary Relocation Initiatives: Potentials, Challenges and Next Steps. (ifa Edition Culture and Foreign Policy). Stuttgart: ifa (Institut für Auslandsbeziehungen).

Recuperado de:

<https://doi.org/10.17901/AKBP1.08.2020>

Annex

I. Recommended resources and guides

DIGITAL SECURITY

Artists at risk connection. Safety Guide for Artists. 2021.

<https://artistsatriskconnection.org/guide/safety-guide-for-artists>

Allied Media Project. Tools and resources for liberation created by the AMP network. <https://alliedmedia.org/resources>

CiviCERT y RaReNet, El Kit Primeros Auxilios Digitales. 2019.

<https://www.digitalfirstaid.org/es>

Digital Defenders Partnership. Digital Integrity Fellowship accompaniment of Civil Society Organizations and Human Rights Defenders. 2019 <https://manuals.digitaldefenders.org/>

Electronic Frontier Foundation. Digital security Companion.

<https://sec.eff.org/>

Front Line Defenders. Guide to Secure Group Chat and Conferencing Tools, 2020. <https://www.frontlinedefenders.org/es/resource-publication/guide-secure-group-chat-and-conferencing-tools>

Front Line Defenders, Protección física, emocional y digital para el trabajo desde casa en tiempos del COVID-19. 2020. <https://www.frontlinedefenders.org/es/resource-publication/physical-emotional-and-digital-protection-while-using-home-office-times-covid>

Privacy International. A guide for migrants and asylum rights organizations about privacy settings. 2019.

<https://privacyinternational.org/act/migrants-asylum-rights-organisations-privacy-settings>.

Privacy tools. <https://www.privacytools.io/>

Tactical Tech. Holistic security. 2016. <https://holistic-security.tacticaltech.org/>

Thomson Reuters Foundation Practical and legal tools to protect the safety of journalists. 2021. <https://safetyofjournalists.trust.org/>

DIGITAL GENDER-BASED VIOLENCE

Access Now Digital Security Helpline End-User Guides. Guide for Safer Online Dating
<https://guides.accessnow.org/safer-online-dating.html>

Cyberwomen. Holistic digital security training curriculum for women human rights defenders. 2018.
<https://cyber-women.com/en/>

Coalition against online abuse. Online Violence Response Hub. 2021
<https://onlineviolenceresponsehub.org/about-the-online-violence-response-hub>

Hackblossom. A DIY Guide to Feminist Cybersecurity. 2018
<https://hackblossom.org/cybersecurity/>

Hollaback. Technical safety guides and Social Media Safety Guides.
<https://iheartmob.org/resources>

Pen America. ONLINE HARASSMENT FIELD MANUAL.
<https://onlineharassmentfieldmanual.pen.org>

RECOMMENDED DIGITAL RIGHTS ORGANIZATIONS

EUTRP and Protect Defenders have produced an international map of digital rights organizations that you can download from the following link:

<https://protectdefenders.eu/wp-content/uploads/2020/07/EUTRP-Mapping-of-Digital-Security-Actors-Supporting-HROs-2021.pdf>



Digital
Defenders
Partnership

www.digitaldefenders.org/es/

calala
Fondo de Mujeres

www.calala.org
calala@calala.org

 @FondoCalala

 @calalafondodemujeres

 @CalalaFondo