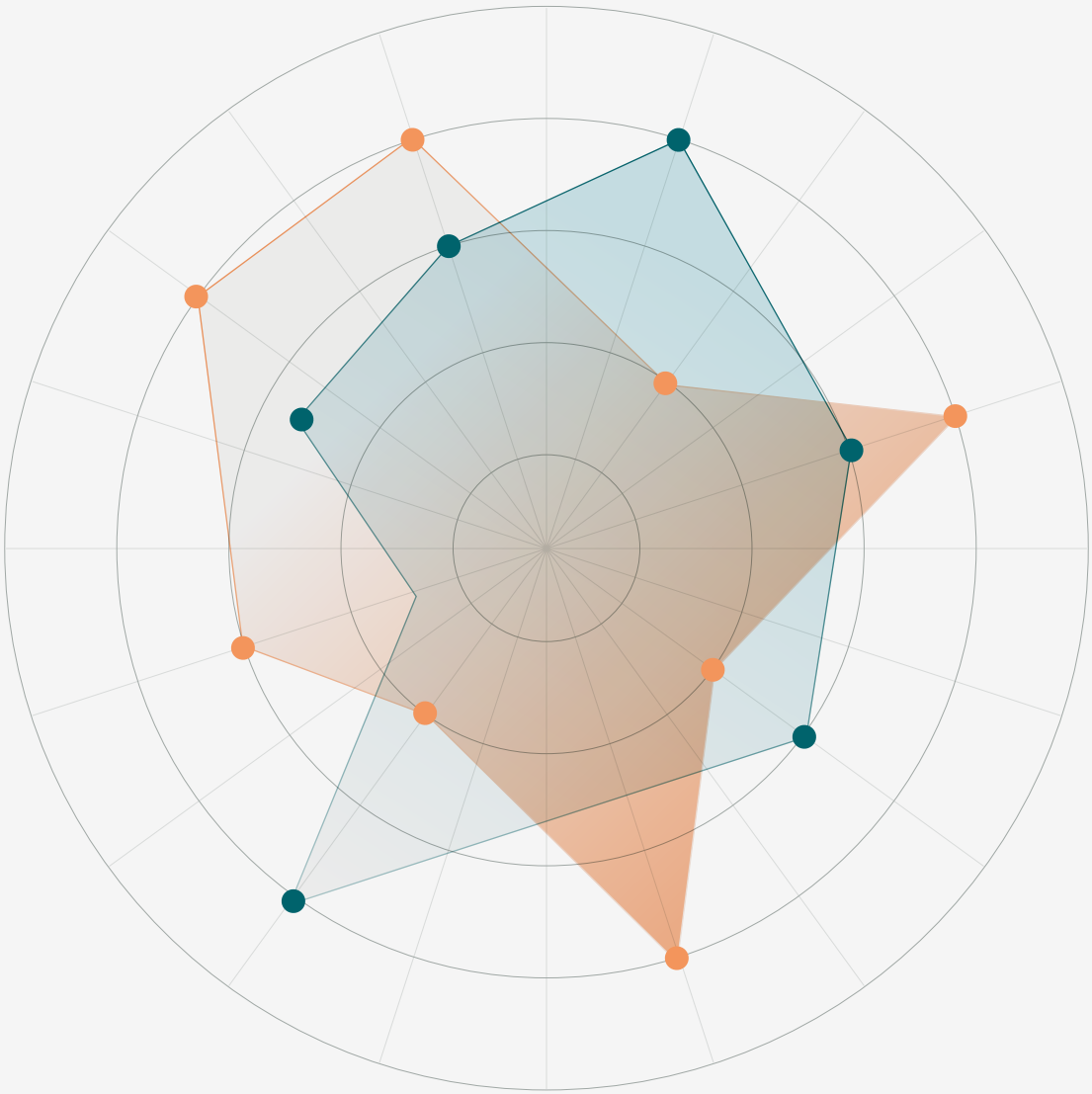
Blueprint

Guidelines for the Development of Information Systems for the Prevention of Crimes Against Human Rights Defenders



CEJIL

CENTER FOR JUSTICE AND INTERNATIONAL LAW

Guidelines for the Development of Information Systems for the Prevention of Crimes Against Human Rights Defenders

July 2026

The Center for Justice and International Law (CEJIL) has as its mission to contribute to the enjoyment of human rights through the effective use of the Inter-American Human Rights System (IAHRS) and other international protection mechanisms.

ISBN 978-987-23854-9-1

Preparation and supervision:

Viviana Krsticevic
Executive Director, CEJIL

Johanna González
Attorney, CEJIL

Franco Albarracín
Attorney, CEJIL

Editorial Design Coordination:

David Romero,
Director of Communications, CEJIL

Nadia Ferrari,
Communications Officer, CEJIL

Design and Layout:

Julieta Melina Jiménez,
Editorial Graphic Designer

How to cite this material:

CEJIL, Guidelines for the Development of Information Systems for the Prevention of Crimes Against Human Rights Defenders. July 2026.

Blueprint

Guidelines for the Development of Information Systems for the Prevention of Crimes Against Human Rights Defenders

CEJIL
CENTER FOR JUSTICE AND INTERNATIONAL LAW

Foreword

Those who defend human rights in the Americas do so, all too often, at the expense of their safety and their lives. Threats, criminalization, surveillance, displacement, and murder have become a daily reality for thousands of people, communities, and organizations that uphold democracy, the rule of law, and human rights in the region. Every attack against a human rights defender not only affects the victim but also weakens societies' ability to demand rights, hold those in power accountable, and preserve an open civic space.

In light of this reality, international and constitutional law have been clear: States have an obligation to prevent, protect against, investigate, punish, and provide reparation for human rights violations. Effective compliance with these obligations requires systems capable of producing, integrating, analyzing, and disseminating information on attacks against human rights defenders. Without reliable, coordinated, and timely information, it is impossible to gauge the magnitude of the phenomenon, identify risk patterns, or guide effective responses for prevention, protection, and investigation.

And yet, the problem is rarely a total lack of data. States, international organizations, academia, and civil society organizations have amassed a vast body of valuable information. The main shortcoming lies in the way this information is organized, linked, and used to guide public policy. These Guidelines aim precisely to provide a roadmap—technical, legal, and methodological—for collecting and transforming that data into an information system capable of strengthening prevention, protection, investigation, and accountability in response to attacks against human rights defenders.

This document is the result of a deeply collaborative and interdisciplinary effort, and it would not have been possible without the generosity of many individuals and institutions.

We would like to extend our special thanks to the Global Rights Innovation Lab Clinic (GRIL) at the University of California, Berkeley—in particular, Laurel Fletcher and Valentina Rozo Ángel—whose contributions, along with those of a brilliant team of students, made possible the interdisciplinary approach that distinguishes this work. Their analyses of criminalization taxonomies, diverse types of information systems, available data sources, and statistical and data science tools significantly broadened the analytical perspectives and enriched the development of this *Blueprint*. We also express our gratitude to experts María Sol Espain and Ari Cunha for their invaluable contributions to the interdisciplinary approach.

We thank the Colombian government institutions that participated in the technical roundtables and shared their expertise and observations, particularly the Office of the Ombudsperson and the Presidential Council for Human Rights and International Humanitarian Law, as well as the Ministry of the Interior, the Attorney General's Office, the Jurisdicción Especial para la Paz (JEP), and the National Environmental Licensing Authority (ANLA, using its Spanish acronym); and to the international organizations that supported the dialogue: UN Women and the Office of the United Nations High Commissioner for Human Rights (OHCHR). We also acknowledge the invaluable contributions of Brazilian state institutions—the Federal Public Prosecutor's Office, the Ministry of Human Rights and Citizenship, the Ministry of Justice and Public Security, and the National Council of Justice—to the debate on the comprehensive protection of human rights defenders and the fight against impunity.

It is equally essential to acknowledge the fundamental contribution of civil society organizations, which—often in a pioneering manner—have documented attacks against human rights defenders. We extend our special thanks to the "José Alvear Restrepo" Lawyers' Collective (CAJAR) and the Somos Defensores Program, whose collaboration proved particularly valuable throughout this entire process. Special recognition is also due to the "No es Hora de Callar" campaign for its decisive role in strengthening information systems in Colombia. We also acknowledge the contributions of the Colombian Commission of Jurists (CCJ), the Foundation for Press Freedom (FLIP, using its Spanish acronym), the Instituto de Estudios para el Desarrollo y la Paz (INDEPAZ), and the Consultoría para los Derechos Humanos y el Desplazamiento (CODHES). In Brazil, we are grateful for the exchanges with the Comissão Pastoral da Terra (CPT), the Coordenação Nacional de Articulação das Comunidades Negras Rurais Quilombolas (CONAQ), the Articulação dos Povos Indígenas do Brasil (APIB), Justiça Global, the National Human Rights Council

(CNDH, using its Portuguese acronym), and the National Council of Traditional Peoples and Communities (CNPCT, using its Portuguese acronym).

We also express our gratitude to the Swiss Agency for Development and Cooperation, the Swedish International Development Cooperation Agency, and the Huneeus Quesney Foundation, whose support made this work possible.

We also thank Dr. Jorge Roa Roa for his academic contributions to this research, as well as those of Dr. Anna Luisa Walter de Santana and Professor Andrea Robles Ustariz, and the comments provided by Dr. Gabriel Rojas Andrade. This work would not have been possible without the exceptional dedication, within CEJIL, of a team committed to researching, drafting, and developing the document presented here, of which I had the privilege of being a part alongside Johanna González and Franco Albarracín. At various stages of the process, we also received support and advice from several colleagues, among whom we would like to highlight—for their sustained contributions—María Noel Leoni, Florencia Reggiardo, and Helena de Souza Rocha. We also benefited from the valuable collaboration of Dayana Mosquera, Vanessa Rossel, and Juan Peltier on logistical and technical tasks.

We hope that these Guidelines will help States, civil society, and academia strengthen the tools, practices, and policies that protect those who defend the rights of all people. Because, ultimately, protecting human rights defenders means strengthening democracy, the rule of law, and the enforcement of human rights.

Viviana Krsticevic

Executive Director, CEJIL

Table of Contents

Glossary of Acronyms

ACHR. American Convention on Human Rights.

CCC. Constitutional Court of Colombia.

CEJIL. Center for Justice and International Law.

GRIL. Global Rights Innovation Lab Clinic, University of California, Berkeley.

HRDs. Human rights defenders.

IACHR. Inter-American Commission on Human Rights.

I/A Court H.R. Inter-American Court of Human Rights.

IAHRS. Inter-American Human Rights System.

ICCPR. International Covenant on Civil and Political Rights.

ICESCR. International Covenant on Economic, Social, and Cultural Rights.

NGO. Non-governmental organization.

OAS. Organization of American States.

OHCHR. Office of the United Nations High Commissioner for Human Rights.

RELE. Special Rapporteur on Freedom of Expression of the IACHR.

SLAPP. Strategic Lawsuits Against Public Participation.

UN. United Nations.

Glossary of Key Terms

Active transparency. The duty of the government to produce and disseminate information on its own initiative—without a request—in a complete, clear, accurate, up-to-date, and timely manner, through accessible channels.

Anonymization. A protective measure that allows information to be processed or published without identifying individuals, by irreversibly removing identifiable data.

Blueprint. Literally, "plan" or "preliminary design" (from the term "blueprint," referring to technical architectural drawings). In this document, it refers to a set of guidelines or reference architecture that translates legal obligations and operational needs into minimum, verifiable parameters for the design, strengthening, and harmonization of information systems on attacks against human rights defenders. It is not an information system or a fixed proposal for technological implementation: it is a guide that can be adopted, adapted, or used as a resource in different national contexts.

Codebook. A supplementary document that defines, for each variable, its conceptual content and coding rules, so that two people coding the same information independently arrive at the same result.

Criminalization. The misuse of criminal, civil, or other branches of law by state and non-state actors with the intent or result of inhibiting, restricting, or silencing the defense of human rights through the manipulation of the state's punitive power.

Data repository. A shared environment that centralizes information from multiple sources while preserving the identity of each database, without consolidating it into a single analytical database.

Early warning. A preventive alert regarding a risky situation. It may be structural in nature—referring to medium-term risk factors—or imminent—when the risk is about to materialize— (in the Colombian case).

Integrated database. A single analytical database that consolidates information from multiple sources—after a deduplication process—and allows for the estimation of underreporting. It is the most robust option for identifying patterns and trends—because it cross-references all the information in a single database—and also the most demanding in terms of integration and standardization.

Interoperability. The ability of different information systems to exchange and use data with one another, based on common structures, definitions, and formats.

Macro-criminal approach. An approach that views incidents not as isolated events, but in terms of networks of responsibility, chains of command, and patterns that link individuals, groups, and institutions.

Memorialization. Processes of constructing memory regarding serious human rights violations, recognized by international standards as a guarantee of non-repetition.

Metadata. Technical information associated with each data point (source, date of entry and update, verification method and level, sensitivity, person responsible for uploading, etc.) that ensures its traceability.

Multiple Systems Estimation (MSE). A statistical method that estimates underreporting—cases not documented by any source—based on the degree of overlap among sources that record the same cases.

Predictive model. A data science tool that, based on the historical behavior of variables, estimates the probability of future events or identifies patterns of escalation (for example, through logistic regression or case clustering).

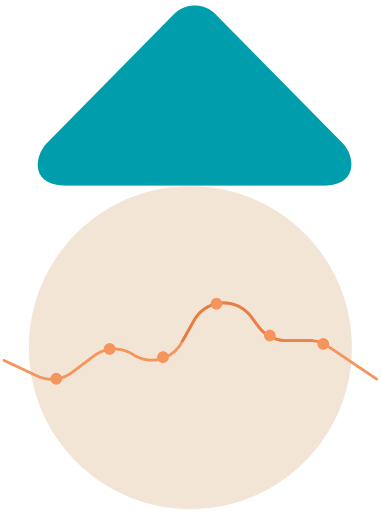
Record deduplication / linkage *(record linkage)*. A process that prevents the same incident or victim from being counted twice when reported by multiple sources, by identifying when different records correspond to the same case. It can be deterministic (exact match of identifiers) or probabilistic (estimating, based on various variables, the probability that two records correspond to the same case).

Standardization. The establishment of equivalence rules between preexisting categories and new variables, which allows for the harmonization of historical data recorded using different definitions or formats.

Structured / semi-structured / unstructured database. Types of databases based on their degree of organization: structured databases are organized into rows and columns; unstructured databases consist of text, audio, or video without a tabular format; semi-structured databases combine both. Predictive models can work with all three, although unstructured databases require preprocessing.

Traceability. The ability to determine, for each piece of data, its origin, the time it was entered, who recorded it, and its verification status throughout its entire life-cycle. It is based on the metadata associated with each piece of data.

Underreporting. The gap between the events actually documented and the actual total number of cases. Its existence justifies the use of statistical methods for estimation and cross-validation between sources.



I. Introduction: Information Systems for Prevention, Protection, and Accountability in Response to Crimes Against Human Rights Defenders

This document proposes guidelines for the development of information systems for prevention, protection, accountability, and reparation in response to attacks against human rights defenders (hereinafter HRDs). Its development responds to the obligation of States to produce systematic, reliable, and useful information on the situation, attacks, and risks faced by those who exercise the right to defend human rights. This is a fundamental element for strengthening public policies to address violence and preserving an open civic space for the defense of human rights.

This document is based on a central premise: information on attacks against human rights defenders only serves a protective function if it allows us to move beyond the isolated recording of incidents to the identification of patterns, risks, institutional responses, and responsibilities. Therefore, information systems should not be viewed as mere repositories of cases, but rather as a fundamental tool of state policy to fulfill its due diligence obligations regarding prevention, protection, investigation, and accountability.

The state's obligation to produce information on violence against human rights defenders stems both from commitments made at the international level and from

constitutional mandates. Thus, the United Nations Declaration on Human Rights Defenders (1998) establishes the state's duty to create the conditions for the free and safe exercise of human rights defense work[1] . Similarly, the Regional Agreement on Access to Information, Public Participation, and Access to Justice in Environmental Matters in Latin America and the Caribbean (hereinafter, the Escazú Agreement) reaffirms the central importance of protecting a safe and conducive environment for the exercise of rights and of guaranteeing the rights of human rights defenders in environmental matters[2]. At the inter-American level, this obligation stems from the state's duty to respect and guarantee human rights, prevent foreseeable risks, protect individuals and groups in situations of vulnerability, investigate acts of violence, punish those responsible, and provide reparation for rights violations. The Inter-American Court of Human Rights (hereinafter the Inter-American Court) has expressly recognized the value of the work of human rights defenders for democracy and the rule of law, as well as the right to defend human rights. Furthermore, the Court has confirmed the existence of enhanced obligations on the part of States toward human rights defenders[3] and, as a corollary to these obligations, has determined since 2021 the need to establish national information systems on human rights defenders in the cases *of Bedoya Lima et al. v. Colombia* (2021)[4] , *Sales Pimenta v. Brazil* (2022)[5] , and *CAJAR v. Colombia* (2023)[6]. In the case of Colombia, the Constitutional Court has reinforced these requirements in a significant ruling on the situation of human rights defenders[7] .

---

1 General Assembly. Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms, Resolution A/RES/53/144, 1998.

2 Escazú Agreement, Article 9.

3 Inter-American Court of Human *Rights. Case* of *Escaleras Mejía et al. v. Honduras*, Judgment of September 26, 2018, Series C No. 361, para. 54; Inter-American Court of *Human* Rights. *Case of Human Rights Defender et al. v. Guatemala*, Judgment of August 28, 2014, Series C No. 283, para. 142

4 Inter-American Court of Human Rights. *Case of Bedoya Lima et al. v. Colombia*, Judgment of August 26, 2021, Series C No. 431, para. 193.

5 Inter-American Court of Human Rights. *Case of Sales Pimenta v. Brazil,* Judgment of June 30, 2022, Series C No. 454, para. 178.

6 Inter-American Court of Human Rights. *Case of Members of the "José Alvear Restrepo" Lawyers' Collective v. Colombia*, Judgment of October 18, 2023, Series C No. 506, para. 1047.

7 At the domestic level in Colombia, Judgment SU-546 of 2023 by the Colombian Constitutional Court (hereinafter CCC) and its Clarifying Order No. 845 of 2024 mandated, in a structural ruling on an unconstitutional state of affairs (hereinafter ECI), the coordinated implementation of a database on community leaders and human rights defenders and the launch of a computerized early-warning system.

These obligations and orders converge on a common requirement: to develop information systems capable of strengthening the protection of human rights defenders and civic space. Within this framework, States must proactively produce systematic information—and, where relevant, georeferenced data—that makes it possible to assess the scale of the phenomenon of harassment, identify patterns of aggression through appropriately disaggregated data, recognize risk factors and territorial contexts, guide prevention and protection measures, monitor the institutional response, support effective investigations, and contribute to non-repetition. Furthermore, these systems must incorporate adequate safeguards to protect the privacy and confidentiality of personal data; guarantee the integrity and digital security of sensitive information; facilitate interoperability among entities; and ensure mechanisms for the effective participation of human rights defenders and civil society in their design, implementation, and evaluation.

The guidelines proposed here aim to translate international obligations and standards into concrete institutional, technical, and methodological design criteria for information systems on attacks against human rights defenders. They do not seek to replace existing information systems, impose a single model, or define a one-size-fits-all solution applicable uniformly to all national contexts, or all institutions tasked with collecting information on this phenomenon. On the contrary, the proposal seeks to outline the minimum elements that a system of this nature should include, taking into account international standards[8], a review of existing national and international experiences in this area, and a fruitful dialogue with institutions, civil society organizations, and experts.

Meeting these standards requires a macro-level architecture capable of coordinating sources, generating logical relationships and risk models, and producing useful inputs for the prevention, protection, investigation, punishment, and reparation of the various forms of violence against human rights defenders. At times, this results

8 See section 3 of the document. For example, the IACHR maintains that an information system must contain: "Data on the number of convictions obtained and the degree to which all those responsible have been identified, including direct perpetrators, intellectual authors, or indirect perpetrators, as well as accomplices, with statistics disaggregated by type of attack (homicide, disappearance, threats, displacement) and by population group (human rights defenders who are women, LGBTIQ+ individuals, Indigenous people, and people of African descent, as well as environmental, community, and JAC defenders), with verifiable annual targets for improvement." IACHR. *Second Report on the Follow-up to Recommendations: Situation of Human Rights Defenders and Social Leaders in Colombia*, OAS/Ser.L/V/II, Doc. 7/26, February 3, 2026, para. 242.

in multiple databases that enrich our understanding of the phenomenon, such as those produced by civil society and international institutions, which offer nuances and counterpoints to some of the official databases and data.

Developing a national-level information system on human rights defenders through the use of multiple databases or systems is not without its challenges. It is necessary to determine to what extent it is possible to coordinate these sources while taking into account their legal frameworks and specific characteristics, preserve their autonomy, identify overlaps, reduce duplication by combining their use, and produce useful information without creating forced centralization or increasing risks to human rights defenders. Comparative experiences in the management of sources can provide valuable insights for addressing these challenges, especially considering that, for regulatory and institutional reasons, multiple sources of information on the phenomenon and a plurality of databases often coexist[9]. The technical discussion on the most appropriate architecture for contexts with multiple sources—including the option of progressive database integration—is developed further below, in the section on the basic elements of an information system[10].

These guidelines draw on the study of some existing information systems. In particular, they build on the experience of Colombia, with a complementary look at Brazil and insights from global and comparative experiences. The case of Colombia is significant for this exercise because the commitment to address the severity and persistence of violence against human rights defenders in the country has led to one of the most developed ecosystems in the region in terms of records, databases, and documentation mechanisms produced by public entities, civil society organizations, independent observatories, and international organizations. Also relevant are the policies, institutional developments, and even judicial oversight aimed at addressing the persistent phenomenon of attacks against human rights defenders, social leaders, and journalists[11]. This experience allows for a more precise analysis of some of the challenges related to coordination, interoperability, traceability, data quality, and the legitimate use of data, as well as the type of data processing, products, and

9 In this regard, it is possible that public prosecutor's offices, national human rights institutions, and human rights organizations may have relevant databases.

10 See section 5 of the document.

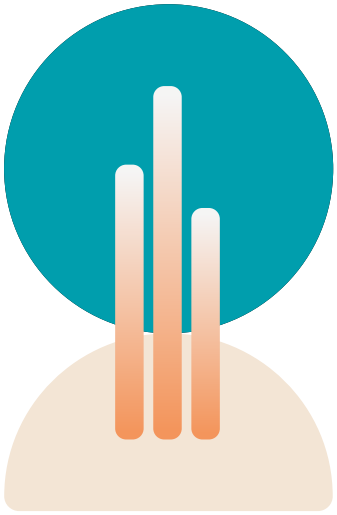
11 Constitutional Court of Colombia (CCC). Ruling SU-546/23, December 6, 2023. Order No. 24; CCC. Order 845-24, May 9, 2024.

interfaces needed to maximize their impact—without assuming that all countries in the region start from the same point—.

The development of these guidelines is based on a rigorous and collaborative methodological process. The process included documentary research on international standards, a review of academic and open-source information, interviews with institutions and organizations, technical roundtables, and the active involvement of experts[12]. The design of the categories and variables was based on an analysis of open-source materials and a comparative study conducted by the *Global Rights Innovation Lab Clinic* (GRIL) at the University of California, Berkeley. Furthermore, during the course of the research, we were supported by a team and three data science experts who contributed to our analysis and made it possible to develop two models. This process included the empirical verification of the alignment between current registration practices and applicable legal standards. This allowed us to identify both the structural similarities among existing systems and the recurring gaps that a new architecture must address.

The *Blueprint* is organized into 12 sections. First, it outlines the reasons why an information system of this nature is necessary and the strategic functions it must fulfill. Next, the objectives of the Guidelines are elaborated. Then, the legal basis underpinning the proposal is specified. Further on, the basic elements of an information system are presented, followed by the substantive categories that structure the proposed architecture. Subsequently, the aspects to be considered for data management are addressed, and the analytical and operational uses of the information system are outlined. Thereafter, the possible results or *outputs* are presented, and the institutional and civil society interfaces are elaborated upon. Toward the end, the ethical principles that should guide both the design and the day-to-day operation of the system are outlined, and the governance guidelines necessary for its implementation and sustainability are established. Finally, the conclusions are presented.

12 For this investigation, the relevant Colombian databases of the following entities were analyzed—through interviews, formal information requests ("derechos de petición"), meetings, and primary sources: the Ombudsperson's Office ; the Ministry of the Interior; the Attorney General's Office (FGN); the National Environmental Licensing Authority (ANLA); the Special Jurisdiction for Peace (JEP); the Presidential Office for Human Rights and International Humanitarian Law; the Somos Defensores Program; Indepaz; and the Office of the United Nations High Commissioner for Human Rights (OHCHR).



II. The Need for an Information System on Human Rights Defenders

Violence against human rights defenders (HRDs) constitutes one of the most serious challenges to democracy, the rule of law, and the effective enforcement of fundamental rights in the region. The most recent reports from specialized organizations—using different methodologies and scopes of coverage—document a sustained trend of lethal and non-lethal attacks against them, as well as the erosion of the enabling environment for the protection of rights[13]

These reports highlight the dire situation in Colombia, Mexico, Guatemala, Brazil, Honduras, and Peru, where persistent patterns of lethal and non-lethal violence are intertwined with disputes over territorial control, the presence of armed groups and illegal economies, socio-environmental conflicts, institutional weakness, and, in

13 Mary Lawlor, Special Rapporteur on the situation of human rights defenders. *Report to the Human Rights Council, A/HRC/61/40, January 5, 2026, para. 1;* IACHR. *Third Report on the Situation of Human Rights Defenders in the Americas*, OAS/Ser.L/V/II, Doc. 119/25, April 15, 2025, p. 8; Global Witness, *Defenders Annual Report 2025: Roots of Resistance*, 2025. Available at: https://gw.hacdn.io/media/documents/Defenders_Annual_Report_2025_online_EN.pdf; Front Line Defenders. *Global Analysis 2025/26*, 2026. Available at: https://www.frontlinedefenders.org/sites/default/files/fld_ga_2025-26_digital.pdf. The HRD Memorial is a joint initiative of a network of human rights organizations that includes Amnesty International, FIDH, Front Line Defenders, Global Witness, and the Somos Defensores Program, among others.

certain cases, state action or inaction in the face of foreseeable risks[14]. They also document the shrinking of civic space, the continued criminalization of human rights defenders, and the continued detention of political prisoners in several countries in the hemisphere, notably in Venezuela, El Salvador, and Nicaragua[15].

The monitoring mechanisms of the Universal System and the Inter-American Human Rights System (hereinafter IAHRS) confirm that the environment for exercising the right to defend human rights remains highly strained in Latin America—a region that accounts for the vast majority of killings of human rights defenders globally—[16] due to a set of mutually reinforcing structural factors: the weak or absent comprehensive presence of the State in the most affected territories or among significant segments of the population[17]; direct State action or omission as a causal or aggravating factor of vulnerability, including the inadequacy of existing protection mechanisms[18]; the stigmatization and criminalization of human rights defenders

---

14 IACHR. *Third Report on the Situation of Human Rights Defenders in the Americas,* OEA/Ser.L/V/II, Doc. 119/25, April 15, 2025; Mary Lawlor, Special Rapporteur on the Situation of Human Rights Defenders. *Report to the Human Rights Council, A/HRC/61/40, January 5, 2026;* IACHR. *Second Follow-up Report on Recommendations: Situation of Human Rights Defenders and Social Leaders in Colombia,* OAS/Ser.L/V/II Doc. 7/26, February 3, 2026; Global Witness, *Defenders Annual Report 2025: Roots of Resistance*, 2025. Available at: https://gw.hacdn.io/media/documents/Defenders_Annual_Report_2025_online_EN.pdf; Front Line Defenders. *Global Analysis 2025/26,* 2026. Available at: https://www.frontlinedefenders.org/sites/default/files/fld_ga_2025-26_digital.pdf..

15 United Nations High Commissioner for Human Rights. *Situation of human rights in the Bolivarian Republic of Venezuela (advanced unedited version),* A/HRC/59/58, June 26, 2025, paras. 33–52; United Nations High Commissioner for Human Rights. *Situation of human rights in Nicaragua*, A/HRC/60/92, pp. 4–5; IACHR. *State of Emergency and Human Rights in El Salvador*, June 28, 2024, para. 391; IACHR. *Situation of Human Rights in Guatemala*, OEA/Ser.L/V/II, Doc. 227/25, November 2, 2025, paras. 183–194.

16 UN. *The Sustainable Development Goals Report,* 2025, p. 41. Available at: https://unstats.un.org/sdgs/report/2025/The-Sustainable-Development-Goals-Report-2025.pdf; Mary Lawlor, Special Rapporteur on the situation of human rights defenders. *Report to the Human Rights Council, A/HRC/46/35, December 24, 2020,* paras. 5, 41.

17 Mary Lawlor, Special Rapporteur on the situation of human rights defenders. *Report to the Human Rights Council, A/HRC/58/53, January 3, 2025,* paras. 5, 47.

18 Mary Lawlor, Special Rapporteur on the situation of human rights defenders. *Report to the Human Rights Council, A/HRC/46/35, December 24, 2020,* para. 9.

by State and non-State actors[19]; high levels of impunity in the face of attacks[20]; increasing forms of digital violence, surveillance, and online espionage[21]; the distinct risks faced by women human rights defenders and indigenous, Afro-descendant, and peasant human rights defenders[22]; the presence of non-state armed actors who exercise territorial control through illicit economies[23]; and conflicts linked to the extractive development model and the failure to resolve historical disputes over land and territory, as well as structural inequality[24], among others.

However, the capacity to document these phenomena varies significantly across the region. While some countries have relevant databases produced by state entities, intergovernmental organizations, civil society organizations, or academia, others lack even basic records of information. Even when they do exist, some of these databases function as passive records, focusing primarily on lethal incidents; while others record crimes without identifying those committed against human rights defenders.

Properly documenting attacks against human rights defenders and the shrinking of civic space is necessary as it is complex. Without adequate and timely information, it is impossible to understand the magnitude of the phenomenon, identify risk patterns, guide prevention and protection measures, or evaluate the effectiveness of the state's response. Part of this complexity stems from at least four factors: (i)

---

19 IACHR. *Third Report on the Situation of Human Rights Defenders in the Americas*, OEA/Ser.L/V/II, Doc. 119/25, April 15, 2025, p. 8.

20 IACHR. *Third Report on the Situation of Human Rights Defenders in the Americas*, OEA/Ser.L/V/II, Doc. 119/25, April 15, 2025, p. 7; Michel Forst, Special Rapporteur on the Situation of Human Rights Defenders. *Report to the United Nations General Assembly.* A/74/159, July 15, 2019, paras. 23, 24

21 IACHR. *Third Report on the Situation of Human Rights Defenders in the Americas*, OAS/Ser.L/V/II, Doc. 119/25, April 15, 2025, p. 134; Michel Forst, Special Rapporteur on the Situation of Human Rights Defenders. *Report to the United Nations General Assembly.* A/74/159, July 15, 2019, para. 21.

22 IACHR. *Third Report on the Situation of Human Rights Defenders in the Americas*, OEA/Ser.L/V/II, Doc. 119/25, April 15, 2025, pp. 8, 36, 47; Mary Lawlor, Special Rapporteur on the Situation of Human Rights Defenders. *Report to the Human Rights Council, A/HRC/46/35, December 24, 2020,* paras. 54, 66.

23 IACHR. *Third Report on the Situation of Human Rights Defenders in the Americas*, OEA/Ser.L/V/II, Doc. 119/25, April 15, 2025, p. 7.

24 IACHR. *Third Report on the Situation of Human Rights Defenders in the Americas*, OEA/Ser.L/V/II, Doc. 119/25, April 15, 2025, p. 7, Mary Lawlor, Special Rapporteur on the Situation of Human Rights Defenders. *Report to the Human Rights Council, A/HRC/46/35, December 24, 2020,* paras. 10.

underreporting; (ii) the variety of types of violence; (iii) the collective nature of human rights defense; and (iv) the diversity of definitions, documentation strategies, and reporting outputs.

To begin with, there is a high degree of complexity involved in thoroughly documenting human rights violations. Both state entities and civil society organizations have varying capacities for documentation, territorial networks, and financial resources. Consequently, it is to be expected that there will be multiple sources yielding different results, and that some may not even record crimes against human rights defenders as a specific category—which makes it difficult to identify or link events and contributes to the underreporting of such violations—. In this context, cross-checking and the use of statistical methods are necessary to understand the scope of the problem[25].

Second, some of the existing documentation systems record homicides but do not necessarily capture—or do so with the same rigor—the broader range of violations suffered by human rights defenders. These include threats and attacks, forced displacement, confinement, arbitrary detention, disappearances, public shaming and stigmatization, criminalization through the misuse of criminal law, impunity for the attacks suffered, sexual violence, and, increasingly, symbolic, and digital violence[26]. Nor do they necessarily capture the geographical prevalence of these incidents, the diversity of forms of violence, barriers to institutional access, or the use of formal and informal mechanisms of persecution[27].

Third, some of the records tend to document individual incidents without accounting

---

25 For example, in the case of Colombia, in 2016, six entities and organizations (Indepaz, Programa Somos Defensores, Cumbre Agraria, Front Line Defenders, OHCHR, and the Ombudsperson's Office) monitored the killings of social leaders, with individual figures ranging from 61 to 133 cases. By cross-referencing and consolidating the six lists—without counting the same case twice (through a deduplication process)—160 murders were documented. Using statistical methods to estimate the total number of cases, it was found that this figure could range from 160 to 180, with a 95% confidence interval. In other words, there could be up to 20 murdered leaders who were not documented by any organization. See: Patrick Ball, César Rodríguez Garavito, and Valentina Rozo. *Murders of Social Leaders in Colombia in 2016–2017: An Estimate of the Total Number of Cases.* Bogotá: Dejusticia, August 2018.

26 UN Human Rights. *Situation of Human Rights Defenders in Colombia (2022–2025).* Bogotá: Office of the United Nations High Commissioner for Human Rights in Colombia, March 2026.

27 IACHR. *Third Report on the Situation of Human Rights Defenders in the Americas,* OEA/Ser.L/V/II, Doc. 119/25, April 15, 2025.

for linked violations or their collective scope. For example, they may record the murder of an indigenous leader without considering the series of acts of harassment suffered by his or her community or by his or her lawyers. Consequently, rights violations are rarely reflected with the comprehensiveness that the phenomenon demands[28]. Moreover, in some cases, the available records capture only a fraction of the problem or were used in the past as tools of persecution[29]. This leads to reluctance to share useful or necessary information with certain state actors.

Fourth, in cases where relevant information is available, the diversity of definitions and documentation strategies constitutes, in and of itself, a valuable feature of the information ecosystem: it reflects the plurality of mandates, approaches, and territorial ties of those who document, and has made it possible to shed light on realities that would otherwise have gone unrecorded. Thus, the challenge does not lie in diversity itself, but rather in the fact that it hinders the ability to make the necessary connections between the collected data to generate the analyses and products required by international and national mandates—both at the individual level and in an aggregated manner by integrating the various databases. Additionally, even in well-developed databases, data processing and its results could be improved to generate more appropriate and timely information and analysis for decision-making.

By using various categories, serving diverse purposes, and applying heterogeneous verification methods, the various systems face serious interoperability obstacles, which make it difficult to construct consistent historical time series, identify common patterns, and produce coordinated responses among authorities with overlapping jurisdictions or confidentiality obligations. Thus, although the multiplicity of records is a necessary condition for rigorously measuring the magnitude of the phenomenon, the absence of mechanisms to integrate them and make them comparable prevents the full utilization of this wealth of information to generate

---

28 UN Human Rights. *Situation of Human Rights Defenders in Colombia (2022–2025)*. Bogotá: Office of the United Nations High Commissioner for Human Rights in Colombia, March 2026.

29 Consequently, the IACHR states that "(...) it calls on the State to address the observations regarding possible inconsistencies between data from different entities and to strengthen inter-institutional coordination to bridge these gaps. Similarly, it urges the establishment of mechanisms to prevent information from being used for improper monitoring or profiling of human rights defenders. Consequently, it is essential to move toward a unified, reliable registry that includes civil society participation, in accordance with inter-American standards of due diligence, prevention, and protection." IACHR. *Second Follow-up Report*, OEA/Ser.L/V/II, Doc. 7/26, 2026, para. 103.

the accumulated knowledge required for the effective protection of human rights defenders. Added to this is the fact that strengthening data processing capabilities and producing timely and adequate results can enhance both individual systems and the aggregate analysis of the whole. At times, a lack of attention to the interfaces between existing systems weakens protection and justice mechanisms, with repercussions for the State's capacity to prevent or impose sanctions.

These difficulties are evident even in the region's most developed information systems. Colombia offers an illustrative case in this regard. Precisely because it has one of the most extensive and diverse documentation ecosystems in the hemisphere, it was possible to conduct a systematic mapping of a set of relevant databases from nine civil society organizations and state institutions. The study showed that information on human rights defenders exists, albeit in a fragmented manner: of the databases analyzed, none exceeds 41% of variables with structured and quantifiable data[30]. Among the main gaps identified are the limited coverage of information on criminalization, mental health, and psychosocial risks faced by human rights defenders, digital repression, technological surveillance, and the use of intrusive software. In addition, limitations were observed in the information and comparability of data on alleged perpetrators and levels of responsibility, as well as in the traceability of protective measures and their effectiveness, and in territorial and

30 In its investigation, GRIL analyzed nine sources of information: (i) the *Early Warning System (SAT)* and the *Follow-up Report on Early Warning 026-18* from the Ombudsperson's Office; (ii) the Ministry of the Interior's *Index of Special Zones of Guarantees for Social Leadership*; iii) the *Human Rights Defenders Bulletins* and the *public report* submitted by the Office of the Attorney General in compliance with paragraph 19 of Constitutional Court Ruling SU-546 of 2023; iv) the National Environmental Licensing Authority's (ANLA) *Characterization of Human Rights Defenders in Environmental Matters and Socio-Environmental Organizations*; v) the reports *Analysis of the Human Rights and Security Situation in Colombia: Impacts of the Ceasefires and Total Peace* and *Severity of the Human Rights Situation in Colombia* by the Special Jurisdiction for Peace (JEP); vi) the *Information Module on Homicides of Social Leaders and Human Rights Defenders* from the Presidential Office for Human Rights; vii) the semi-annual and annual reports of *the Information System on Attacks against Human Rights Defenders in Colombia (SIADDHH)* from the Somos Defensores Program; viii) the *Monitor of Assassinations of Social Leaders and Human Rights Defenders in Colombia* and the report *"A Deadly Trend: The State's Failure to Protect Social Leaders"* by Indepaz; and ix) the *Situation of Human Rights in Colombia (Report of the High Commissioner)*, along with the infographic and the presentation of the OHCHR's *2021–2025 Annual Report of the High Commissioner*. For the analysis, 14 categories were defined: (i) data management, (ii) demographics, (iii) alleged perpetrators, (iv) type of attack, v) type of aggression—criminalization, vi) health, vii) risk factors, viii) territorial context, ix) socioeconomic and political context, x) rule of law, xi) institutional protection measures, xii) prosecution indicators, xiii) administrative and public policy response, xiv) monitoring and evaluation, with more than 80 variables.

population-based disaggregation.

The gaps identified in the Colombian case highlight how the fragmentation of information, along with difficulties in integrating it and producing adequate results, can constitute a specific form of informational impunity. The guidelines proposed here aim to help overcome these challenges and demonstrate why this effort is extremely valuable and indispensable.

That said, recognizing the need for information systems on human rights defenders and taking into account the challenges they face, it is important to clarify their strategic objectives or functions. First, to strengthen early risk prevention by identifying trends, recurring patterns, and warning signs. Second, to improve individual, collective, and territorial protection by enabling the prioritization of cases, the adjustment of measures, and the monitoring of their effectiveness. Furthermore, such systems should contribute to the investigation and prosecution of incidents, facilitate the monitoring of impunity, inform the State's criminal policy, and provide evidence for the formulation, monitoring, and evaluation of public policies. Finally, it should serve as a tool for accountability and as an interface with academia, civil society, affected communities, and processes of memory, truth, and reparations. All of this must be carried out in accordance with the principles of legitimate use and precaution, which prevent data collection for the purposes of persecution or stigmatization.

1

Early Risk Prevention

Enables the identification of escalations, recurring patterns, and warning factors to take action before major harm occurs.

2

Enhancing Individual, Collective, and Territorial Protection

Helps prioritize cases, adjust protection measures, and monitor their effectiveness to safeguard lives and territories.

Information Systems on Human Rights Defenders

Data to protect, prevent, and guarantee rights

3

Investigation and Prosecution of Incidents

Facilitates the collection and preservation of evidence, strengthens investigations, and supports bringing perpetrators to justice.

4

Evidence-Based Public and Criminal Policy

Generates actionable information to formulate, monitor, and evaluate public policies, while enabling tracking of impunity levels and institutional responses.

5

Accountability and Social Engagement

Serves as an accountability tool and an interface connecting academia, civil society, affected communities, and memory, truth, and reparation processes.

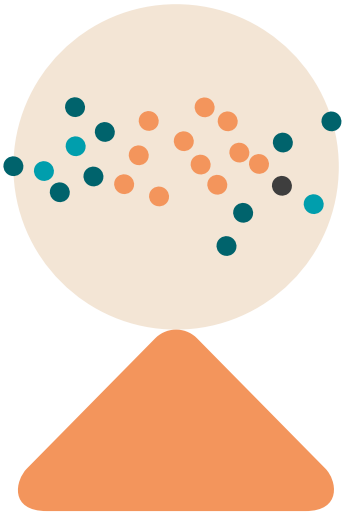
Under Principles of Legitimate Use and Precaution

Legitimate Use:
Exclusively for protection, prevention, investigation, and public policy purposes.

Precaution:
Minimising risks of exposure and potential harm.

Confidentiality:
Safeguarding personal data and ensuring confidentiality.

Non-Discrimination:
Prohibiting stigmatisation, discrimination, and persecution.



III. The Objectives of the Blueprint

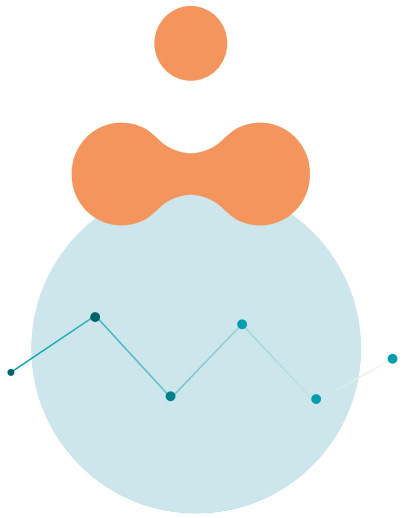
The *Blueprint* consists of a set of guidelines designed to guide and support the processes of building, strengthening, and harmonizing information systems on attacks against human rights defenders, using the guidance and standards of international human rights law as a reference. It constitutes a reference architecture that translates legal obligations and operational needs into verifiable parameters for institutional design, and can be adopted, adapted, or used as a resource by States, protection bodies, and civil society organizations responsible for producing or coordinating information on this phenomenon. The *blueprint* is neither an information system nor a closed proposal for technological implementation. Rather, it seeks to identify a set of minimum common elements that will strengthen the quality, comparability, interoperability, and public utility of the information produced in different national contexts. The strategy is to harmonize standards and propose outcomes to maximize the effectiveness of systems, not to replace existing information systems or impose uniform formats.

Given the plurality of state, independent, community, and multilateral sources, the goal must be to preserve that diversity and build upon it an architecture capable of linking sources, generating meaningful associations between data, and improving interoperability. This is clearly evident in Colombia, where multiple registries coexist with different logics, methodologies, purposes, and scopes, featuring the gaps we highlighted above and lacking sufficient mechanisms for coordination among them. In other national contexts, the challenge may be different, as rather than coordinating existing sources, it may be necessary to create basic registries where

violence against human rights defenders is not yet systematically documented or recorded with regard to the victim's status or other factors required under international law. In this regard, in Brazil, for example, government documentation of homicides and other human rights violations does not typically identify victims based on their status as human rights defenders, which makes it difficult to adequately assess the scale of the phenomenon. Therefore, these guidelines should be interpreted and implemented in accordance with the conditions, capacities, and needs of each country and the entities carrying out this work.

In general terms, this document defines the minimum content that must be included in the data architecture and information systems. It also provides guidance on the incorporation and coordination of diverse sources; proposes rules for quality, verification, and the avoidance of duplication; identifies essential system functionalities; sets out guidelines for analyzing the information and developing the minimum public-interest products it generates—statistics, periodic reports, maps, early warnings, and case narratives—; incorporates appropriate safeguards for the protection of sensitive information; and provides an initial framework for system governance, including mechanisms for the participation of defenders, affected communities, and civil society. Rather than merely promoting the collection of information, the *blueprint* seeks to create conditions for transforming data into useful knowledge for prevention, protection, investigation, and the formulation of evidence-based institutional responses.

More specifically, the proposed design aims to improve the regional comparability of records, facilitate risk analysis, strengthen coordination among public entities with overlapping jurisdictions, reduce informational impunity, and expand public access to information relevant to participation, protection, and the exercise of rights. It also seeks to ensure that the information produced through data processing and analysis—as well as the products derived from it—is useful for prevention, the investigation of events, truth, justice, and reparations processes, and the formulation of public policies. The goal is to create conditions so that government decisions regarding prevention, protection, investigation, and reparation can be evaluated, and so that affected communities can use more transparent and useful tools to defend their rights. Ultimately, the objective is for the information system to cease functioning as a passive record of events and become an active infrastructure for the effective guarantee of the right to defend rights.



IV. The Creation of Information Systems is an International Legal Obligation of States

The development of an information system on attacks against human rights defenders is not merely a matter of good public policy practice; it is also supported by positive legal obligations derived from international human rights law and national constitutional developments, as discussed above. These obligations define the substantive and procedural parameters that must guide the design and operation of databases intended to document, analyze, and prevent violence against human rights defenders.

At the universal level, the United Nations Declaration on Human Rights Defenders (1998) expressly recognizes the right of every person, individually or collectively, to promote and seek the protection and realization of human rights and establishes the state's duty to create the conditions for the free and safe exercise of human rights defense work[31]. This instrument incorporates obligations already enshrined in numerous universal human rights treaties related to the exercise of the right to defend human rights. Among them are the International Covenant on Civil and

31 General Assembly. Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms, Resolution A/RES/53/144, 1998.

Political Rights (ICCPR) and the International Covenant on Economic, Social, and Cultural Rights (ICESCR)[32].

At the Inter-American level, we highlight primarily the American Convention on Human Rights (hereinafter ACHR) and the Escazú Agreement, from which state obligations arise that express the enhanced protections deserved by human rights defenders and the protection of an enabling environment for the exercise of human rights.

Thus, the case law and legal doctrine issued by the Inter-American Court of Human Rights (I/A Court H.R) and the thematic reports of the Inter-American Commission on Human Rights (hereinafter IACHR) have established specific standards applicable to the protection of human rights defenders and the right to defend human rights. In particular, the Inter-American Court of Human Rights has progressively developed standards regarding the collection, systematization, dissemination, and safeguarding of information related to attacks against human rights defenders, particularly through the guarantees of non-repetition ordered in the *Bedoya Lima, Sales Pimenta*, and *CAJAR* cases, as well as in the findings of the *Zapata* case and Advisory Opinion No. 32/25.

In the Judgment *in Bedoya Lima et al. v. Colombia*, the Inter-American Court ordered the State to design and implement, within one year, a system for collecting data and statistics on violence against journalists, with an emphasis on gender-based violence against women journalists. The measure included the collection of indicators on judicial proceedings—, indictments, convictions, and acquittals—and the periodic dissemination of that information with the necessary safeguards to protect the victims' identities[33]. In the case *of Sales Pimenta v. Brazil*, the Inter-American Court replicated and expanded the measure to include environmental and land defenders, requiring an assessment of "the type, prevalence, trends, and patterns of violence" and the disaggregation of data by state, ethnic origin, political

---

32 Human Rights Committee, *General Comment 34: Freedom of Opinion and Freedom of Expression (Article 19 of the ICCPR)*, CCPR/C/GC/34 (2011), paras. 21–36; and Human Rights Committee, *General Comment 36: The Right to Life (Article 6 of the ICCPR)*, CCPR/C/GC/36 (2019), para. 7; Committee on Economic, Social and Cultural Rights, *Statement: Human Rights Defenders and Economic, Social, and Cultural Rights*, E/C.12/2016/2, March 29, 2017, para. 5.

33 Inter-American Court of Human Rights. *Case of Bedoya Lima et al. v. Colombia*, Judgment of August 26, 2021, Series C No. 431, para. 193.

affiliation, gender, and age[34]. It also ordered the creation of a working group to identify the causes of structural impunity associated with these attacks[35] In the *CAJAR v. Colombia* decision, the Inter-American Court of Human Rights consolidated the standard within the framework of a structural judgment and expressly linked the production of information to the duties of prevention, protection, and non-repetition. The Court held that the absence of comprehensive information prevents an adequate assessment of the magnitude of violence against human rights defenders, the identification of risk patterns, and the design of effective public policies to address the phenomenon[36].

This line of reasoning was further developed in *Advisory Opinion 32/25* on the climate emergency and human rights. There, the Inter-American Court of Human Rights clarified that the production of information constitutes a state obligation derived from the right of access to information[37]. Consequently, States must collect and maintain up-to-date disaggregated data on murders, kidnappings, enforced disappearances, arbitrary detentions, torture, and other harmful acts against environmental defenders[38]. Furthermore, States are required to take into account socioeconomic factors, as well as gender, age, sex, and ethnicity, and to design policies aimed at addressing the structural causes of violence, incorporating an intersectional approach that allows for the identification of and response to the differentiated impacts resulting from situations of discrimination and vulnerability[39].

It should be noted that, in the *Zapata* case (2025), the Inter-American Court of Human Rights recognized the duty of States to adopt the necessary measures to protect the integrity and security of systems that store personal data against

---

34 Inter-American Court of Human Rights. *Case of Sales Pimenta v. Brazil,* Judgment of June 30, 2022, Series C No. 454, para. 178.

35 Inter-American Court of Human Rights. *Case of Sales Pimenta v. Brazil,* Judgment of June 30, 2022, Series C No. 454, para. 145.

36 Inter-American Court of Human Rights. *Case of Members of the "José Alvear Restrepo" Lawyers' Collective v. Colombia*, Judgment of October 18, 2023, Series C No. 506, para. 1047.

37 Inter-American Court of Human Rights. *Advisory Opinion OC-32/25*, May 29, 2025. Series A No. 32, para. 505.

38 Inter-American Court of Human Rights. *Advisory Opinion OC-32/25*, May 29, 2025. Series A No. 32, para. 575.

39 Inter-American Court of Human Rights. *Advisory Opinion OC-32/25*, May 29, 2025. Series A No. 32, para. 575.

unauthorized access and undue interference, with special attention to the collection and storage of data on human rights defenders[40].

The *Escazú Agreement* added a particularly significant dimension for the region by strengthening obligations regarding access to information, public participation, environmental justice, and special protection for environmental defenders. This treaty recognizes in its provisions the importance of ensuring an enabling civic space and the relevance of environmental defenders, their protection, and the investigation of crimes committed against them, in order to ensure the rights to sustainable development and to the environment. The Action Plan on Human Rights Defenders in Environmental Matters, adopted under the *Escazú Agreement,* includes knowledge generation as one of its priority areas (Area A)[41]. The Plan requires States to conduct assessments of the situation of those who promote and defend human rights in environmental matters, including the number of victims and the types of violations, instruments for prevention, protection, and punishment, early warning systems, and community-based self-protection practices and strategies[42]. These measures take on particular relevance in contexts where attacks are linked to conflicts over land, natural resources, infrastructure, or land use, and where the information asymmetry between the State, companies, and communities acts as a risk-aggravating factor.

40 Inter-American Court of Human Rights. Case of *Zapata v. Colombia*, Judgment of October 3, 2025, Series C No. 569, para. 154.

41 ECLAC. *Action Plan on Human Rights Defenders in Environmental Matters in Latin America and the Caribbean and its Implementation Program*, LC/ESZ.2025/4, 2026, pp. 11–12, 14–16.

42 ECLAC. *Action Plan on Human Rights Defenders in Environmental Matters in Latin America and the Caribbean and its Implementation Program*, LC/ESZ.2025/4, 2026, pp. 11–12, 14–16.

Based on the guidance provided by the inter-American standards and the Escazú Agreement, a set of minimum guidelines emerges for the design of information systems on attacks against human rights defenders regarding content, purpose, outputs, and operating conditions[43].

In terms of content, these systems must record not only homicides or other lethal attacks, but also threats, disappearances, displacements, arbitrary detentions, torture, harassment, criminalization, digital violence, surveillance, attacks against organizations, and other forms of violence or restrictions on the exercise of the right to defend human rights. They must also capture not only isolated individual incidents but also their collective dimension—whether through the victim's organizational or community affiliation or through sequences of attacks directed against groups, communities, or organizations. This information must be disaggregated, at a minimum, by type of attack, territory, victim profile, gender, age, ethnicity, type of work, group affiliation, risk context, alleged perpetrator, and possible state action or omission. The disaggregation of information is not merely a methodological issue, but a substantive requirement for highlighting distinct risks and specific patterns of violence that disproportionately affect women human rights defenders, indigenous peoples, Afro-descendant communities, rural communities, environmental defenders, journalists, and other groups in situations of vulnerability.

As for the purpose, the use of information should not be limited to the retrospective recording of completed lethal incidents. It should make it possible to assess the magnitude of the phenomenon of attacks, identify patterns of violence, recognize risk factors, analyze structural causes, implement prevention and protection

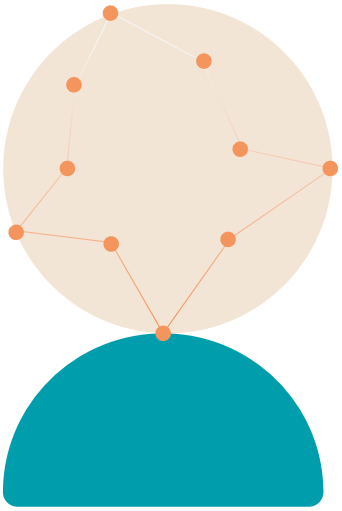
43 It should be noted that the consolidation of these standards at the international level is now finding concrete expression in the Colombian case. The Constitutional Court of Colombia (CCC), in Ruling SU-546 of 2023 and Order 845 of 2024, declared the security situation facing community leaders and human rights defenders to be unconstitutional. This declaration was based on the persistent and widespread violation of their fundamental rights, as well as on the State's insufficient institutional and budgetary capacity to guarantee their protection. In response, the Court issued two orders directly related to the production and management of information. First, it ordered the coordinated implementation by various agencies of a single database—defined as an information system composed of various existing databases—designed to register community leaders and human rights defenders. This database must include comprehensive statistics and coordinated management of information regarding the types of violence suffered by this population, based on a uniform definition of a human rights defender and in accordance with the principles of habeas data. Second, the court ordered the implementation, within six months, of a responsive and efficient digital communication system (such as webchat, WhatsApp, or a mobile app) that allows citizens to report threats and risks to their lives and physical integrity, with immediate verification and urgent activation of protective measures.

measures, evaluate their effectiveness, guide research, monitor levels of impunity, and contribute to truth, reparations, and non-repetition.

In terms of outputs, these systems must generate statistical data, periodic public reports, visualization dashboards, maps, alerts, trend analyses, pattern studies, predictive models, and other useful inputs for institutional and social decision-making. The dissemination of this information must be carried out with the necessary safeguards to protect the identity, safety, and privacy of victims where appropriate.

Finally, regarding their operating conditions, these systems must be accessible to various audiences—authorities, civil society, academia, affected communities, and mechanisms for protection, justice, truth, and reparations—without losing sight of the principles of security, confidentiality, participation, consent, legitimate use, and do no harm. The production of information on human rights defenders serves as a protective function only if it avoids undue profiling, surveillance, stigmatization, or any use that increases the very risks it seeks to prevent.

Case / Standard	Bedoya Lima et al. v. Colombia	Sales Pimenta v. Brazil	CAJAR v. Colombia
Type of victim	Female journalist and defender of freedom of expression.	Enviromental and land defenders.	Human rights organization and its members.
Pattern of violence analyzed	Sexual violence as a mechanism of indirect censorship and silencing.	Lethal and non-lethal violence against defenders in the context of territorial disputes and structural impunity.	Illegal surveillance, stigmatization, threats, and assassination attempts as a systematic policy.
Legal classification of violence	Sexual violence = serious violation of human rights + indirect restriction on freedom of expression.	Violence against human rights defenders = violation of the right to life and physical integrity with a reinforced duty of prevention.	State violence and surveillance = multiple violations with direct state responsibility.
Duty to Investigate	Enhanced due diligence with a gender-sensitive approach, focusing on cases related to journalistic practice.	Serious investigations, conducted within a reasonable timeframe, aimed at dismantling impunity.	Enhanced investigations, including analysis of patterns and state responsibility.
Use of State Power/Force	Prohibition on tolerating or permitting sexual violence as a form of control or punishment.	State liability for omission in the face of foreseeable risks.	Prohibition on the use of the state apparatus (intelligence, surveillance) to persecute human rights defenders.
Information system (express order)	Express order to create a national data system (1 year).	Express order to create a national data system (2 years).	Express order to create a national data system (1 year).
Function of the data system	To record sexual violence, indirect censorship, and gender-based violence for prevention purposes.	To assess the true magnitude of violence and guide public policy.	To measure patterns, judicial proceedings, oversight of state power, and non-repetition.
Required disaggregation	Gender-based approach (women journalists).	Territory, ethnicity, political affiliation, gender, and age.	Territory, scope of action, gender, and other differential approaches.
Judicial proceedings indicators	Implicit (impunity as a form of censorship).	Indictments, convictions, and acquittals.	Investigations, indictments, convictions, and acquittals.
Publicity and personal data	Enhanced protection of the victim's dignity and privacy.	Annual publication with identity withheld.	Annual publication with safeguards for personal data.
Guarantees against recurrence	Data system + structural reforms, training, gender-based approach.	Data system + working group against impunity.	Data system + accountability and institutional oversight.
Key contribution to the Inter-American standard	Recognizes sexual violence as a form of indirect censorship and requires a gender-based approach.	Establishes that without data, there can be no prevention or public policy.	Consolidates the information system as an autonomous obligation and a tool for state oversight.



V. Basic Elements of an Information System[44]

Information systems are based on an architecture comprising three essential components: first, the physical infrastructure and servers (*hardware*); second, the programs and algorithms (*software*); and third, the team that designs and operates the processes. The guidelines developed in this document focus primarily on the *software* pillar—that is, the system's programs that enable the management of the data lifecycle—.

For the information system on human rights defenders to fulfill its function, it must have i) a mechanism for high-quality data entry, ii) processing capabilities that allow for the organization and analysis of information, and iii) useful and timely outputs that transform that data into knowledge to guarantee the right to defend rights, prevent and protect against risks and violence, investigate incidents of harassment, its proximate causes, and risk factors, and mitigate and remedy harm.

The effectiveness of information systems depends directly on the quality of the information entered, the decisions made during its processing, and the results produced. In the case of databases related to human rights violations, it is common for them to exhibit biases linked to differing institutional approaches or mandates, difficulties in collecting certain information, and the perspectives of those analyzing

44 We thank the GRIL team at Berkeley for their invaluable contributions to this document, particularly regarding the interdisciplinary sections and the development of the taxonomy on criminalization.

the data, among other factors. Biases can arise because each source—whether from the government, civil society organizations, or other actors—has a limited scope of observation, creating gaps that prevent the available information from being considered a complete representation of the phenomenon. When certain fields are systematically missing or certain cases are never documented, the database ceases to be a neutral representation of the phenomenon and instead reflects inequalities in access, visibility, and power. In this regard, interpreting any results requires understanding how gaps in the entered information can introduce biases that affect the results obtained, and assessing whether the chosen system can mitigate these effects through data processing or whether it simply reproduces them. This highlights the importance of collecting reliable data from diverse sources and providing relevant guidelines for its processing.

The multiplicity of information sources relevant to understanding the phenomena affecting human rights defenders also has implications for the design of the information system. In particular, it requires defining an architecture capable of handling information from diverse sources in a reliable, verifiable, and methodologically robust manner. To this end, two recommended structures are identified: a data repository or an integrated database of a repository.

> The **data repository** option centralizes information from multiple sources while maintaining the original identity of each database. The repository functions as a shared storage and query environment capable of incorporating different types of data—structured databases, reports, maps, or other relevant documents—while preserving the traceability of the original source. This approach facilitates access to, comparison of, and cross-referencing of information from different entities; it allows for the incorporation of indicators and complementary sources to enrich the analysis; and it promotes the protection of sensitive information through anonymization mechanisms and differentiated access controls. However, on its own, this option does not resolve duplications between sources, nor does it allow for the estimation of underreporting, so its analytical capacity is limited.

> On the other hand, the **integrated database of a repository** represents a more advanced level of information integration. Unlike a data repository, it is not limited to simply aggregating various sources but consolidates them into a single analytical database, deduplicating records through linking or deduplication techniques (*record linkage*). This makes it possible to identify when diverse

> sources refer to the same event or the same person (overlaps), while maintaining traceability to the original sources, and to estimate underreporting using statistical methods such as Multiple Systems Estimation[45]. It is the most robust option for analyzing patterns and trends, but also the most demanding in technical, operational, and inter-institutional coordination terms. Generally speaking, it allows us to go beyond what is reported and estimate the total number of cases. This distinction is crucial in contexts where information is fragmented, and there are systematic gaps in the recording of human rights violations.

It should be noted that there is a more basic option: **a new structured or semi-structured database,** that is, a system created from scratch with its own data collection structure. Its advantage is that it allows for standardizing data from the outset and maintaining total control over the variables and data entry processes. However, it is limited to the information that the entity is able to document, reproduces observational biases, and does not allow for estimating underreporting or cross-checking multiple sources. This type of database can be useful in contexts where information is lacking, but in many national situations, there are multiple institutions and organizations that collect relevant information[46]. Therefore, while an in-house database is essential for producing official information, the need to cross-check data and enrich the analysis with diverse sources makes it advisable to opt for a repository or an integrated database.

However, it is worth noting that these options for the structure of the information system are not mutually exclusive. It is possible for an entity or organization to develop a new database, for that database to be incorporated into a repository along with other databases, and for it to form part of an integrated database. Furthermore, regardless of the option chosen, the system's usefulness will depend on the quality of the *input*, the methodological decisions made during processing, and the ability to identify and mitigate issues of bias and underreporting. Additionally, some of the system's potential uses, as well as its scope and quality, will vary depending on

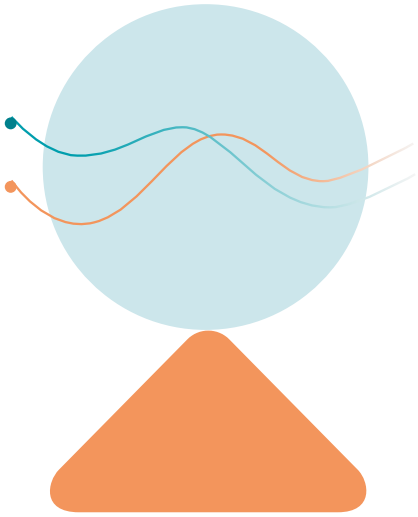
---

45 For examples of states' duty to guarantee the right to the truth and to use statistical methods such as this one, see: Alejandro Jiménez Ospina et al., *Telling the Truth: Statistics in Uncovering Patterns of Violence.* Bogotá: Dejusticia, December 2022.

46 For example, data on homicides, injuries, and ongoing criminal or judicial proceedings concerning attacks against human rights defenders that are conducted by national human rights institutions, ministries responsible for security and justice, prosecutors' offices, truth commissions, non-governmental organizations, and international bodies and agencies, among others.

the level of integration achieved. Within this framework and taking into account the expected functions of the information system for human rights defenders, it is desirable to move progressively toward an integrated database that allows for a better understanding and response to the phenomenon of attacks against human rights defenders, as well as to strengthen prevention, protection, investigation, and accountability measures.

Taking these considerations into account, the following sections outline some of the key elements for designing information systems on human rights defenders, including the substantive categories that should structure the system, the rules for data management and processing, and the analytical and operational outputs that can be derived from the collected information, in light of international standards and comparative practice.



VI. The Categories that Structure the Information System

Based on the objectives of the information system, this section presents a reference framework for the recommended categories and variables. Their selection draws on two sources: on the one hand, international, regional, and domestic standards that identify the elements that any system of this nature must capture; on the other hand, a comparative analysis of a set of existing information systems, reports, and databases in Colombia, as well as some relevant regional experiences[47]. This exercise made it possible to identify both the structural similarities among registries and the recurring gaps that a new architecture can and must address[48].

> Based on these sources, the system is organized around six analytical categories, each addressing a different question: (i) who is the human rights defender; (ii) what acts or omissions affect them; (iii) in what ways is the law being abused against them; (iv) how does the State respond to the situation; (v) who are the alleged perpetrators; and (vi) in what context does the risk arise. Although each category addresses its own specific question, they are designed to function in relation to one another.

47 For more information on the methodology, see Section 1 of the document.

48 It is to be expected that not all databases will document all the variables presented in this section. However, this list corresponds to the key variables identified in the research to analyze and understand the phenomenon of violence against human rights defenders, in light of States' international obligations.

The value of the information system does not lie in the isolated sum of categories or variables, but in the ability to relate them to one another. These categories constitute a minimum foundation that allows for the identification of patterns, the establishment of relevant associations, and the generation of useful knowledge for prevention, protection, investigation, reparations, and guarantees of non-repetition. It is precisely this relational logic that transforms a record of events into a useful tool for decision-making and the formulation of evidence-based institutional responses.

It should be noted that this standard serves as a reference framework and not as a rigid implementation model. Not all jurisdictions need to implement every field from the outset: the proposed set of variables aims to cover the categories currently documented in international standards, comparative registries, and the regional experiences mentioned at the beginning of this document; however, its adoption can be gradual and adapted to the priorities, capacities, and realities of each national or local context.

Below, each of the six analytical categories, their subcategories, and specific variables are outlined. These can be applied to different types of data, including structured, unstructured, or semi-structured data, such as spreadsheets, narrative reports, or complaint forms. Annex I, at the end of the document, presents a consolidated table with the set of proposed categories, subcategories, and variables.

a. Human Rights Defenders

First, the system is built on a broad understanding of *who* human rights defenders *are*. The starting point is the definition of a human rights defender established by the Inter-American Court of Human Rights, based on relevant United Nations developments[49].

It states that:

> "The status of a human rights defender [...] is determined by the very nature of the activities carried out, regardless of whether they are performed on an occasional or permanent basis, in the public or private sphere, collectively or

49 General Assembly. Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms, Resolution A/RES/53/144, 1998.

> individually, at the local, national, or international level, or whether they are limited to specific civil, political, economic, social, cultural, or environmental rights, or extend to all of these"[50] .

Based on this premise, the categories *of human rights defender or victim* do not seek to establish a definitive census, but rather to document events while taking into account those individual and collective characteristics that allow for an understanding of the distinct risks and the identification of the dynamics and patterns associated with the phenomenon, in accordance with the system's objectives, including prevention, protection, investigation of the facts, and reparations for victims. In the context of the Americas, it is particularly important to identify current or past membership in or association with social movements, organizational processes, and non-governmental organizations, among others.

The documentation of each incident of aggression against human rights defenders requires taking into account a series of demographic variables related to their personal and intersectional characteristics, socioeconomic conditions, advocacy work, risk history, and ties to rights defense efforts or organizations. Among the parameters established by international law standards are, among others, sex and gender, age, language, ethnic or racial background, sexual orientation, disability, nationality, immigration status, occupation, profession, education, socioeconomic status, place of residence, place of work, organizational membership, institutional affiliation, political affiliation, type of leadership, and the sector or issue related to their advocacy work[51]. Since several of these variables constitute sensitive data, their inclusion in the system must be accompanied by the safeguards regarding privacy, security, and non-harm detailed in Section Seven.

These variables make it possible to record individual and collective aspects that are important for understanding risk patterns, forms of aggression, and impacts. Of course, the specificity of the categories and the level of disaggregation must be

50 Inter-American Court of Human Rights. Case *of Zapata v. Colombia*, Judgment of October 3, 2025, Series C No. 569, para. 237.

51 See Section 4 of the document. Inter-American Court of Human Rights. *Case of Sales Pimenta v. Brazil*, Judgment of June 30, 2022, Series C No. 454, para. 178; Inter-American Court of Human Rights. *Case of Members of the "José Alvear Restrepo" Lawyers' Collective v. Colombia*, Judgment of June 21, 2023, Series C No. 504, para. 1047; Inter-American Court of Human Rights. *Advisory Opinion AO-32/25 (Climate Emergency and Human Rights)*, May 29, 2025, Series A No. 32, para. 512.

adapted to national or local realities. For example, in Brazil, it is important to identify categories of traditional peoples and communities, such as the *ribeirinha* communities, whose way of life is closely linked to river ecosystems and who play a central role in defending water resources, or the *quilombola* communities —Black communities, both rural and urban, self-identified and characterized by historical and collective ties to their territories, their own forms of social, cultural, and political organization, and histories of resistance to slavery—. Similarly, in Ecuador, it is important to recognize the Montubio people as a distinct category—a coastal peasant community with its own cultural identity, associative forms of organization, and constitutional recognition as a subject of collective rights. Incorporating these categories helps bring light risks, conflicts, and forms of impact that might otherwise remain hidden under more general classifications. Similarly, in countries of the region characterized by significant ethnic and cultural diversity, it is essential to recognize the specific categories of self-identification or the languages of traditional peoples and communities.

b. Events and Types of Attacks

The second substantive dimension involves recording the acts and omissions that constitute attacks against human rights defenders, as well as determining the type of aggression documented.

Attacks are not limited to lethal or physically violent acts, but encompass a spectrum of behaviors that include stigmatization, surveillance, threats, and displacement, as well as other direct attacks and forms of administrative, economic, legal, and digital harassment. This understanding of aggression expressly includes state actions and omissions, because only in this way is it possible to capture the role of the state as a potential perpetrator—whether by directly violating rights or by failing to fulfill its duty to protect when it does not act with due diligence to prevent, investigate, punish, or provide reparation. The analytical value of the registry lies not solely in the isolated identification of an act or omission, but in the possibility of interpreting them within a relational framework. Later on, we will provide further details on data management, minimum metadata requirements, deduplication, safeguards, and processing procedures to ensure their proper use.

The categories used to document the various types of attacks must reflect the diversity of relevant legal frameworks—including international law, criminal law, and constitutional law—as well as emerging patterns of rights violations affecting human rights defenders. These include: homicide, attempted homicide, enforced

disappearance, temporary disappearance, arbitrary pretrial detention, criminalization, bodily injury, torture, cruel or inhuman treatment, gender-based violence, sexual violence, sexual torture, slavery, sexual slavery, forced recruitment, confinement, forced displacement, forced eviction, exile, threats, harassment, intimidation, stigmatization campaigns, discrimination, defamation, incitement to violence, *doxxing*; illegal surveillance, interception of communications, use of spyware or malware, internet *shutdowns*, deactivation of SIM cards, blocking or interruption of instant messaging services, closures or suspensions of organizations, administrative obstacles, indirect restrictions, fines, attacks on headquarters, attacks on communities, damage to communal property, attacks on territories, among others.

That said, one of the recurring patterns of rights violations affecting environmental defenders, indigenous leaders, and journalists is the criminalization or misuse of the State's punitive powers by various actors. However, documenting this category is not straightforward because it involves assessing the use of a legitimate power of the State and because there are discrepancies in how various institutions and organizations approach it. Therefore, the category of criminalization is discussed in greater detail below, with the aim of contributing to its proper conceptualization, documentation, and analysis within the information system.

c. Criminalization

The criminalization of human rights defenders is a common tactic used to silence, discredit, retaliate against, or restrict the ability of human rights defenders to carry out their work[52]. Along these same lines, various protection bodies and specialized organizations recognize this phenomenon as one of the most significant ways of restricting the actions of human rights defenders and civic space[53].

---

52 The IACHR has characterized this as "the misuse of criminal law through the manipulation of the State's punitive power by state and non-state actors with the aim of obstructing their defense work and thereby preventing the legitimate exercise of their right to defend human rights." See: IACHR. *Third Report on the Situation of Human Rights Defenders in the Americas*, OEA/Ser.L/V/II, Doc. 119/25, April 15, 2025, para. 150.

53 IACHR. *Third Report on the Situation of Human Rights Defenders in the Americas*, OEA/Ser.L/V/II, Doc. 119/25, April 15, 2025; IACHR and OHCHR. "Safeguarding Civic Space Means Protecting the Right to Defend Rights," press release, December 9, 2025; Mary Lawlor, Special Rapporteur on the situation of human rights defenders. *Report to the Human Rights Council, A/HRC/61/40, January 5, 2026;* Front Line Defenders. *Global Analysis 2025/26,* 2026. Available at: https://www.frontlinedefenders.org/sites/default/files/fld_ga_2025-26_digital.pdf

The Inter-American Court of Human Rights states that: "the State has a duty to investigate complaints, but this responsibility cannot be misused in such a way that [its] punitive power [...] is used as a tool of persecution, especially given the context of violence against human rights defenders"[54]. However, documenting criminalization can be more complex than documenting other phenomena because it generally involves assessing the possible misuse of powers that, in principle, constitute legitimate expressions of state power for the protection of the rights of other individuals, corporations, or public interests. This is one of the reasons why this phenomenon is among the least documented within the categories of conduct that inhibits the right to defend rights.

In an effort to address this underreporting, we develop an operational definition of the category below and propose a set of subcategories and variables designed to facilitate its documentation within the information system on human rights defenders.

The concept of criminalization is primarily associated with the criminal justice system. However, in practice, the punitive use of the law can also operate through civil liability, administrative law, tax law, and other branches of the legal system. That said, the literature offers various definitions of criminalization. These range from approaches that include stigmatizing rhetoric and disinformation campaigns to those that consider the mere initiation of any legal proceeding against a human rights defender to be sufficient, as well as broader approaches related to strategic litigation against civil society and abusive litigation brought by corporations. Based on these developments and the patterns relevant to human rights defenders, these guidelines adopt a more narrowly defined operational definition of criminalization, classifying other important phenomena under various categories of attacks.

For the purposes of these guidelines, criminalization consists of the misuse of criminal, civil, or other branches of law by state and non-state actors with the intent or result of inhibiting, restricting, or silencing the defense of human rights through the manipulation of the State's punitive power.

The lack of systematic documentation of this category in existing databases on human rights defenders led this *Blueprint* to give special attention to the fields

54 Inter-American Court of Human Rights. Case *of Zapata v. Colombia*, Judgment of October 3, 2025, Series C No. 569, para. 198.

necessary for its proper identification. Indeed, the proposal is to organize the category into three axes that address different aspects of the phenomenon: (i) criminalization *per se,* (ii) abuses of the State's punitive power, and (iii) strategic lawsuits against public participation initiated by private actors or companies.

First, there are a number of situations that constitute criminalization *per se,* in that their mere existence allows the event to be classified within this category without the need for further analysis. Generally speaking, this refers to the application of laws incompatible with the State's international obligations, or to actions directed against a conduct that is categorically protected by international law. These are clear-cut cases in which no further analysis of the context is required to conclude that there has been an abuse of punitive power. This category comprises four subcategories, each with its corresponding variables. The first encompasses the criminalization of conduct protected by freedom of expression, whether through the application of offenses such as contempt, slander, or defamation[55], and other similar forms of conduct[56]. The second subcategory refers to punitive action by the State without a legal basis—that is, cases in which the State initiates or maintains punitive measures without adequate legal justification—. Its paradigmatic example is arbitrary detention following the completion of a sentence. The Working Group on Arbitrary Detention (hereinafter WGAD) classifies as arbitrary any deprivation of liberty for which it is clearly impossible to invoke any legal basis, as occurs when a person is kept in detention after having served their sentence or despite an amnesty law that applies to them[57]. Likewise, the WGAD has held that secret detention and enforced disappearance constitute arbitrary deprivations of liberty *per se*, as far as they lack any legitimate legal basis. The third subcategory is the use of military courts to try

55 IACHR, *Criminalization of the Work of Human Rights Defenders*, OEA/Ser.L/V/II, Doc. 49/15, December 31, 2015, para. 94.

56 General Assembly. Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms, Resolution A/RES/53/144, 1998. Art. 13. The document argues that charging individuals with receiving foreign funding amounts to criminalization, since the solicitation, receipt, and use of resources to promote and protect human rights constitute a recognized right.

57 For this category, the criteria of the United Nations Working Group on Arbitrary Detention (WGAD) are followed. Human Rights Council. *Working Methods of the Working Group on Arbitrary Detention*, U.N. Doc. A/HRC/36/38, July 13, 2017, para. 8 (Category I).

civilians[58]. As a variable, cases heard in military courts in which human rights defenders appear as defendants or witnesses may be considered. Finally, the fourth subcategory encompasses those cases in which a competent international body has already determined the existence of criminalization in the context of reviewing a case or urgent action, as may occur with decisions by the Inter-American Court of Human Rights, the Inter-American Commission on Human Rights (IACHR), the Working Group on Arbitrary Detention (WGAD), or other special procedures or treaty bodies.

Second, a series of conduct is included under the category of abuses of state punitive power. These encompass frequent situations involving the potential illegitimate use of powers that, in principle, constitute legitimate expressions of state power. Unlike cases of criminalization *per se,* these cases typically require a contextual assessment of the available information—whether at the individual or aggregate level—to determine whether criminalization actually exists. This category includes actions that are apparently valid in the exercise of criminal, civil, or administrative powers, but that may function as mechanisms of harassment or as restrictions on the work of the defense. Under this category, it is essential to include: i) the abusive use of investigative and prosecutorial powers—for example, multiple investigations or charges, proceedings based on association or membership, and vague or aggravated charges; ii) the filing of false or unfounded charges; iii) the unjustified delay of proceedings—such as delays, arbitrary sequencing, rescheduling, or late disclosure of charges—; iv) the imposition of disproportionate precautionary measures—such as arbitrary pretrial detention, unreasonable surveillance and searches, and excessive bail, among others; v) the imposition of disproportionate penalties—including excessive fines and the dissolution of organizations; vi) violations of due process—restrictions on the right to defense, obstruction of access to legal counsel, withholding of notifications, or violation of *the principle* of *non bis in* idem; and vii) the abusive use of administrative procedures—such as entry bans into third countries—.

Third, this category includes strategic lawsuits against public participation (SLAPPs) in a strict sense. These are strategic lawsuits filed by companies or other non-state

58 IACHR. *Report on Terrorism and Human Rights*, OEA/Ser.L/V/II.116, Doc. 5 rev. 1 corr., October 22, 2002, paras. 231–232; Inter-American Court of Human Rights, *Case of Radilla Pacheco v. Mexico,* Judgment of November 23, 2009, Series C No. 209, paras. 272–275.

actors that, when examined in light of their purpose, seek to harass, discourage, or prevent the work of human rights defenders, and may lead to a finding of abuse of the judicial process[59]. This type of litigation has proliferated in the region and around the world, accompanying corporate strategies aimed at suppressing whistleblowing or protest and creating a chilling effect on civic space[60]. At times, its deterrent power is linked to the possibility of imposing judgments with millions of damages or seizing the assets of individuals and organizations. Among the most common types of cases in this category are lawsuits for property damage or trespassing in the context of protests or territorial defense; defamation lawsuits and others related to freedom of expression; litigation arising from protests affecting extractive or infrastructure projects; multiple and simultaneous lawsuits; and the abusive use of constitutional remedies to protect fundamental rights against organizations or human rights defenders.

Given that some manifestations of criminalization may overlap with one another and with other dimensions of the system, the operational design must establish clear criteria for classification and to avoid duplication. This is particularly important with regard to incidents that could be recorded simultaneously as harassment, surveillance, stigmatization, digital attack, administrative sanctions, abusive judicial proceedings, or restrictions on the exercise of advocacy work. Ultimately, the system's usefulness will depend on its ability to capture the complexity of the phenomenon without artificially multiplying records or losing analytical consistency.

d. State Response to Risk or Incident

i. Prevention and Protection Responses

One aspect emphasized by the inter-American system is the requirement that the *State's response to a risk* be fully observable within the system—not only in terms of its formal existence but also in terms of its timeliness, adequacy, and substantive

---

59 Business and Human Rights Resource Centre. *SLAPPs in Latin America: Strategic lawsuits against public participation in the context of business and human rights*, 2022. Available at: https://media.business-humanrights.org/media/documents/2022_SLAPPs_in_LatAm_EN_v7.pdf; See also: SLAPPs Database and related resources. Available at: https://www.business-humanrights.org/en/from-us/slapps-database/

60 Business and Human Rights Resource Centre, SLAPPs Database and related resources. Available at: https://www.business-humanrights.org/en/from-us/slapps-database/

effectiveness—[61]. This category must take into account several relevant aspects in the development of the information system.

In practice, assessing the state's response involves an analytical shift. It is crucial to determine whether the state acted, but it is also important to evaluate whether it did so in a timely manner, whether the measure adopted was proportionate and appropriate to the identified risk and to the person or group to be protected, and whether it proved effective in neutralizing the risk.

Risk monitoring can also take place through individual or collective measures or early warning systems designed to address those risks. For example, in the case of the Colombian Ombudsperson's Office, early warnings take on distinctive characteristics depending on whether they are issued as imminent warnings or structural warnings[62] .

Monitoring prevention and protection responses involves covering their entire cycle and carefully documenting the attacks or risks that trigger the measures, as well as those that occur while protection measures are in place, since such events serve as indicators of system failures and as evidence that the duty of prevention is not fulfilled by the mere formal adoption of measures.

To this end, the system should record: the request for protection and the corresponding risk assessment; the response time; urgent measures; individual, collective, territorial, or community protection schemes; precautionary measures—whether domestic or issued by the IACHR—and provisional measures; the periodic review, modification, or termination of the schemes, including the reasons for their withdrawal or termination; safe return; and, across the board, an assessment of the sufficiency, adequacy, and effectiveness of such measures, including attacks that occurred while they were in effect.

Following the same logic, monitoring of institutional early warnings—if available—should be incorporated, including both structural and imminent warnings. Given that the information contained in these instruments is not always linked to specific

---

61 Inter-American Court *of Human Rights. Case of Human Rights Defender et al. v. Guatemala*, Judgment of August 28, 2014, Series C No. 283, paras. 157–158.

62 Republic of Colombia. *Decree No. 2124 of 2017*, December 18, 2017, Official Gazette of Colombia.

cases or individuals, the system should provide a differentiated recording process for territorial, contextual, and prospective sources of risk. This workflow should not force early warnings into the structure of individual records but rather allow for the analysis of territorial, temporal, and contextual units, including the territory covered, the population or group potentially affected, the identified risk factors, the patterns of violence detected, the recommendations issued, the entities responsible for responding, and the actions actually taken. Thus, early warnings would not function as isolated records, but rather as prospective information that can be correlated with the subsequent occurrence of attacks and with the timeliness, adequacy, and effectiveness of the state's response.

ii. Justice and Overcoming Impunity

The component of judicial proceedings *and impunity* is central to assessing the effectiveness of the State's protective or safeguarding intervention. While criminalization reflects an excess of punitive power against those who defend rights, impunity reflects a deficit of that same power in the face of those who attack them. According to the Inter-American Court of Human Rights, this repeated deficit acts as a factor in the recurrence and consolidation of patterns of violence[63].

Therefore, the information system must allow for the recording of various aspects of judicial response to attacks against human rights defenders. These guidelines highlight three such aspects: first, indicators of procedural progress and setbacks; second, those that allow for the recording of the different levels and networks of criminal liability; and, finally, the identification of guarantees of material and formal access to justice. However, depending on the issues affecting human rights defenders, it may be necessary to develop categories that go beyond the criminal justice response and allow for the evaluation of other avenues of justice or protection of rights, such as constitutional protection of rights or tutela proceedings, and the effectiveness of civil justice, among others. Nevertheless, given the importance that criminal proceedings typically hold in the pursuit of justice, these guidelines primarily address the variables related to that category.

63 Inter-American Court of Human Rights. *Case of Sales Pimenta v. Brazil,* Judgment of June 30, 2022, Series C No. 454, para. 170.

To begin with, it is essential to map out the entire procedural history of each case—its advances and setbacks—and to link each milestone to the corresponding procedural deadlines, in order to assess compliance with the reasonable time limit. The standard of due diligence and reasonable time established by the Inter-American Court of Human Rights implies the need to record, at a minimum, a series of categories: complaints, investigations that have been opened or are ongoing, indictments, convictions, appeals, final convictions, actual imprisonment, and acquittals. It should be emphasized once again that, depending on the nature of the case, the course of the proceedings may not follow the stages of criminal proceedings; for example, in situations where protection depends on civil lawsuits, constitutional protection actions, or other constitutional remedies.

Additionally, the Inter-American Court's case law requires the establishment of various types of perpetrations and participation in the human rights violations it finds. This includes determining the direct and intellectual perpetrators, investigating chains of command, and identifying various actors who finance, assist, or act with acquiescence in the crime, as well as the levels of planning[64]. Such categories must be expressed in accordance with the traditions of national or comparative criminal law of the relevant country[65] .

Finally, a more comprehensive system should also incorporate indicators capable of identifying the accessibility of justice mechanisms and the broader institutional conditions that influence the institutional response to impunity. In this regard, it is possible to assess whether the potential causal link between the incident and the advocacy work was considered, whether the investigation included a contextual analysis of the associated risks and patterns, or the type of punishment imposed. To this must be added aggregate indicators on the functioning of the justice system, such as its independence and impartiality, the autonomy of investigative and adjudicative bodies, the existence of specialized prosecutors' offices or units, institutional capacity—including the number and training of investigators, caseload, and

64 Inter-American Court of Human Rights. *Case of Manuel Cepeda Vargas v. Colombia*. Judgment of May 26, 2010. Series C No. 213, paras. 119, 216,

65 Inter-American Court of Human Rights. *Case of Manuel Cepeda Vargas v. Colombia*. Judgment of May 26, 2010. Series C No. 213, para. 216.

allocated resources—and levels of corruption[66] To this must be added performance indicators that serve as a tool for accountability in the face of structural impunity, such as delays in proceedings and official statistics on case resolution[67]

e. Alleged Perpetrators

The identification of *alleged perpetrators and networks of responsibility* is an essential analytical category for understanding the risks faced by human rights defenders and breaking cycles of impunity. Their inclusion in the system does not constitute a prejudgment of individual responsibility or a determination of guilt. For the purposes of the system, networks of responsibility include both individual alleged perpetrators and the organizations or groups—whether legal or illegal—to which they belong, as well as institutions that may be linked to crimes or harassment against human rights defenders. This allows investigations to be approached from a macro-criminal perspective when appropriate.

The information system must enable the identification of patterns associated with individuals, groups, and institutions, distinguishing between state agents, non-state actors, and corporate actors, among others. This distinction is legally relevant because, in accordance with inter-American and universal standards, the State is liable not only for the direct conduct of its agents but also for the acts of private individuals when there is acquiescence, tolerance, or a failure to fulfill the duty of due diligence[68].

Among the subcategories that the system should cover are, first, state actors, such as judges, prosecutors, members of law enforcement, public officials, and local authorities, among others. Second, non-state actors, including organized armed groups, various illegal groups, paramilitary groups, or other criminal structures

---

66 IACHR. *Guarantees for the Independence of Justice Officials. Toward Strengthening Access to Justice and the Rule of Law in the Americas*, OEA/Ser.L/V/II, Doc. 44, December 5, 2013, paras. 15–37, 49; IACHR. *Corruption and Human Rights: Inter-American Standards*, OEA/Ser.L/V/II, Doc. 236, December 6, 2019, para. 288

67 IACHR. *Third Report on the Situation of Human Rights Defenders in the Americas,* OEA/Ser.L/V/II, Doc. 119/25, April 15, 2025, paras. 183–185

68 Inter-American Court of Human Rights. *Case of Velásquez Rodríguez v. Honduras*, Judgment of July 29, 1988, Series C No. 4, paras. 172–174.

to be defined based on local, national, regional, and global dynamics[69], as well as individual non-state actors. Third, legal entities or business actors, including corporations, companies, contractors, and third-party funders[70]. Finally, the system should make it possible to identify the forms of coordination among actors, such as mixed arrangements, criminal subcontracting, or the joint action of networks that combine state and non-state actors.

The systematic recording of these variables makes it possible to identify recurring patterns by type of actor, recognize territories and sectors particularly affected by specific forms of violence, and assess the State's compliance with its obligations regarding prevention and punishment.

f. Context

Context is an indispensable dimension of the system because many risks faced by human rights defenders only make sense when viewed against the structural backdrop in which they occur. A homicide, a threat, or a digital attack, when considered in isolation, may seem like unrelated incidents, but when cross-referenced with other variables—rurality, the presence of legal and illegal armed actors, illicit economies, socio-environmental conflict, extractive or infrastructure megaprojects, environmental permitting processes, institutional weakness, historical impunity, or electoral cycles—they reveal sectoral patterns of persecution, differentiated impacts across the territory (municipalities, regions, or transnational dynamics), and their evolution over time.

The information system must enable connections between individual incidents, diverse types of attacks, and structural risk environments. This relational analysis should make it possible to identify the impact of three types of elements: structural variables, patterns, and predictors of violence or vulnerability.

---

69 For example, see: United Nations Office on Drugs and Crime (UNODC), *Global Study on Homicide 2023. Homicide and Organized Crime in Latin America and the Caribbean,* 2023. Furthermore, in an effort to map criminal networks operating regionally, the *Amazon Underworld* project—a collaboration between InfoAmazonia, Armando.info, and La Liga Contra el Silencio—identifies some of the networks relevant to transnational phenomena by mapping the presence of armed groups and criminal economies in the border regions of the Amazon (Bolivia, Brazil, Colombia, Ecuador, Peru, and Venezuela). Available at: https://amazonunderworld.org/map/

70 In this regard, see: Business and Human Rights Resource Centre, SLAPPs Database, and related resources. Available at https://www.business-humanrights.org/en/from-us/slapps-database/

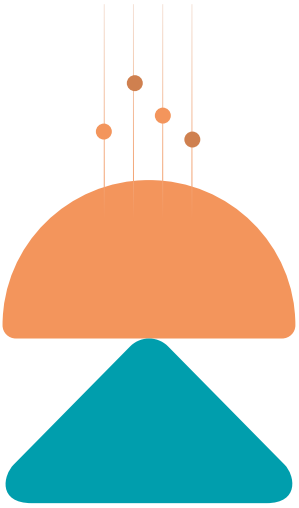
Structural variables could include, for example, areas of particular conflict, the absence of state presence, the presence of legal or illegal armed groups, illicit economies, and levels of corruption—measured, for example, through the Corruption Perceptions Index[71] —, socioeconomic data on the region, rates of violence—such as homicide, femicide, injuries, massacres, kidnapping, sexual violence, human trafficking, forced recruitment, and slave labor—and educational indicators, such as school enrollment and dropout rates.

Regarding the identification of patterns, the system should take into account dynamics relevant to advocacy work in the area, which may affect it directly or indirectly. For example, patterns of enforced disappearance, persecution, confinement, forced recruitment, deforestation, and impunity, among others. It should also identify complex patterns that emerge only from cross-referencing different sources and variables. For example, combining variables on the presence of armed groups, illicit economies, homicide rates, and school dropout rates can reveal recruitment risks in areas where there are no direct reports. Similarly, data from one source may highlight underreporting in another; while the analysis of territorial corridors—extending beyond municipal boundaries—can reveal dynamics of expansion, control, and territorial disputes that help identify the victimization of human rights defenders in specific territories.

In addition, in-depth knowledge of certain phenomena can help identify predictors of violence: indicators with predictive value for clarifying dynamics, adjusting institutional responses, and preventing future acts of aggression. Some of these indicators will depend on the phenomena being documented and on the analytical information produced through qualitative studies, which can then feed into predictive models. These indicators can be expressed through observable events as well as indirect indicators or significant gaps in information. For example, internet shutdowns have been identified as predictors of escalations in violence, including massacres and episodes of police repression worldwide. Other possible predictors include sudden, mass population displacements; electoral contexts; environmental permitting processes in countries with weak institutions; and disputes between illegal armed groups.

71 For more information, see: https://www.transparency.org/en/cpi/2025

This capacity for contextual analysis is a necessary condition for the state to prevent foreseeable risks, investigate incidents, punish those responsible, and ensure reparation for victims.



VII. Data Management

Data management is central to the validity, reliability, and usefulness of the information system. Decisions regarding how each record is identified, described, linked, protected, and preserved determine whether the system will be traceable, interoperable, reliable, secure, and, above all, whether it will be useful for prevention, protection, investigation, accountability, reparations, and guarantees of non-repetition. This section specifies the common rules that apply across all categories: the *codebook* and coding rules, minimum metadata requirements, deduplication criteria, data standardization, normalization, and interoperability, and safeguards to protect information from misuse or risks.

For the purposes of data management, it is important to distinguish between the different types of information processed by the system, which correspond to the categories outlined in the previous section. Each type requires a different approach in terms of metadata, deduplication, and level of protection.

Sources do not always provide information at the same level of detail. The comparative mapping shows that some contain individual records or records of specific incidents, while others present aggregated information, periodic reports, narrative reports, or analytical documents. Therefore, the system must clearly distinguish between required, recommended, conditional, and not applicable fields. When a field cannot be filled in, the system must differentiate the cause using statuses such as “Not applicable,” “Not available”—the data might exist but was not captured—and “Not verifiable”—the data exists but has not met the verification threshold—. This distinction helps avoid confusing the lack of data in a source with the absence of the problem being documented.

a. Codebook and Coding Rules

The codebook is a supplementary document—typically a table or a set of tables—that defines, for each variable captured by the system, its conceptual content, and the rules for coding it. At a minimum, each system's codebook should include the conceptual definition of each variable, its data type, the permitted values when the variable is categorical, the rules for resolving ambiguous values, examples of typical and borderline cases, and the specific criteria for distinguishing, for each variable, between the states "Not applicable," "Not available," and "Not verifiable" mentioned above.

Unlike the consolidated table presented in Annex I, which serves as a reference catalog of variables, the codebook is specific to the particular system implemented by each organization or entity and reflects its operational decisions. Its function is twofold: to ensure internal consistency during coding—so that two people independently coding the same information arrive at the same result—and to serve as a reference for anyone who subsequently consults the database, enabling them to understand what each variable represents, what criteria were applied, and how to interpret the recorded values.

In contexts where the system combines diverse sources or where coding is performed by different teams, the codebook is essential for ensuring that the resulting database remains consistent and comparable over time. When definitions or categories evolve, the codebook must be updated with version control, and that information can be incorporated as metadata within the registry to preserve historical traceability. Furthermore, the existence of a codebook in each implementation is a prerequisite for the regional comparability sought by this *Blueprint*: without detailed documentation of the rules each system applies, interoperability between registries is limited to the mere nominal matching of categories.

b. Minimum Metadata

Minimum metadata consists of the technical information that ensures the traceability of the record and, with it, its auditability, and its ability to be linked with other sources. At a minimum, each record in the system should include: a unique record identifier, which distinguishes each entry from every other entry in the system; an event identifier, which allows multiple records to be associated with the

same incident when different sources report the same assault; the data source, understood as the institutional, organizational, or community origin from which the information comes, preserving traceability back to the original document or system; date of entry and last update, with version control that records subsequent corrections without erasing the chain of custody; status, method, and level of verification, which documents not only whether the data was verified, but also how and with what degree of reliability; authorship or person responsible for the upload, which identifies the individual or unit that entered or modified the record; the data's sensitivity level and access classification, as metadata associated with the record itself—not just with the general category—so that the protection rule accompanies the data throughout its entire lifecycle; and the capture method, which indicates whether the record was manually entered, automatically extracted, or generated through *record linkage* between sources.

It is worth noting that a single system may have more than one observation unit. While the most common record level is the incident, it may also be the human rights defender, organizations, judicial proceedings, or protective measures. Each of these units should have its own unique persistent identifier—for example, a victim, a victim-incident pair, a judicial proceeding, or a protective measure—in addition to the unique record identifier and the event identifier mentioned above. These identifiers are what allow the various tables to be linked together and enable the relational and longitudinal analyses discussed later.

Metadata serves both technical and legal functions. It provides information on where each data point comes from, when it was entered, who recorded it, and its verification status. This traceability is key to evaluating the information in investigations, protective measures, legal proceedings, or proceedings before international bodies, as well as to reviewing how the system operates and detecting potential errors, biases, or misuse of the information.

c. Deduplication Keys

Deduplication is the process that prevents the double counting of the same incident or the same victim when multiple sources report the same event. Deduplication keys are the variables or combinations of variables that the system uses to perform this comparison—for example, name, date, or municipality—. When the source is an aggregated index or an analytical document without

individual records, this field is marked as "Not applicable," since there are no individual units to cross-check[72]

When the volume of records is high or there are typographical errors, names spelled differently, or incomplete information, an exact text match is insufficient, and probabilistic record linking is required. This method evaluates several variables collectively—for example, name, date, location, and victimizing incident—and estimates the probability that two records correspond to the same case. Therefore, the definition of deduplication keys must be adopted alongside safeguards—pseudonymization and access control—and recognized as a conditional field, dependent on the type of source and the system model adopted. Finally, the analysis of the deduplication keys yields unique identifiers for victims and/or victimizing events.

d. Data Standardization, Normalization, and Interoperability

The gradual adoption of this structure requires standardization and normalization rules for managing existing historical information, since not all entities record the same variables, use the same definitions, or store data in comparable formats. To this end, the system should include data dictionaries, common catalogs, equivalence rules between pre-existing categories and new variables, quality criteria, and minimum metadata that allow for determining the origin, scope, update date, verification method, and sensitivity level of each data point. Likewise, an institutional process for updating parameters should be established, allowing for the addition, modification, or removal of variables when the dynamics of violence, conflict, or persecution so require, while preserving the traceability of changes and historical comparability[73].

The automated integration of information among entities with responsibilities for prevention, protection, investigation, and prosecution depends on the existence of standardized data structures, common dictionaries, standardized catalogs,

---

72 Commission for the Clarification of the Truth, Coexistence, and Non-Repetition (CEV), Special Jurisdiction for Peace (JEP), and Human Rights Data Analysis Group (HRDAG). *Methodological report of the joint JEP-CEV-HRDAG project on data integration and statistical estimation*, August 2, 2022, Section 3 "Linkage of Records," pp. 23–24.

73 DANE-SEN. *Recommendations on Mechanisms, Standards, and Protocols for Interoperability in the Exchange, Use, and Reuse of Data in the National Statistical System (SEN)*, May 2025, Dimension 3 "Classifications and Vocabularies," p. 37

minimum metadata requirements, and secure exchange protocols. The technical development of these standards—including controlled vocabularies, metadata schemas, exchange formats, common identifiers, quality rules, and criteria for updating variables—should be addressed in complementary technical guidelines or in a technical annex on interoperability, to be developed during the implementation phase of each national system[74].

e. Safeguards and Data Protection

Safeguards and data protection are essential to the legitimacy, security, and usefulness of the system. In this regard, the collection, storage, processing, and dissemination of data must never increase the risk to human rights defenders or expose their families, communities, organizations, witnesses, or sources. Data protection thus serves as a technical expression of enhanced due diligence and as a safeguard against persecution, surveillance, improper profiling, or stigmatization.

The system should distinguish, at a minimum, between public, restricted, and confidential data, assigning different rules for processing, retention, and dissemination to each level. Categories such as the human rights defender's identity, precise location, physical or mental health status, ethnic or organizational affiliation, sexual orientation or gender identity, or the identity of witnesses and sources must be treated at the highest levels of protection. It should be noted that this governs the processing and dissemination of data at the individual level. It does not prevent—and, in fact, the system must enable—access to aggregated statistical information disaggregated by those same variables—gender, age, ethnicity, type of work, territory, among others—which is precisely what makes it possible to highlight differentiated risks and patterns of violence.

The classification of data determines the applicable protection measures. These include anonymization and pseudonymization, which allow information to be published without identifying individuals and restrict access to identifiable data to authorized parties, through differentiated profiles and for legitimate, explicit, and proportionate purposes. Added to this are data minimization, identity protection,

---

74 DANE-SEN. *Recommendations on mechanisms, standards, and protocols for interoperability in the exchange, use, and reuse of data in the National Statistical System (SEN)*, May 2025, Section 6.2 and Appendix A, pp. 43–50.

and, where applicable, informed consent—understood as a complementary safeguard and not as a substitute for the other protective measures—.

Finally, the security of the system must be demonstrable through specific accountability and oversight mechanisms. These include access logs, which reveal who accesses what information and for what purpose; response protocols for data breaches or security incidents; and periodic human rights and data protection impact assessments, designed to verify that the rules governing classification, access, and dissemination remain proportionate to the system's purposes. Along the same lines, when the system incorporates analytical or predictive tools, oversight becomes even more important. Algorithms can help guide protection or public policy decisions, but these must also take into account human assessment and other relevant sources of information.

VIII. Analytical and Operational Uses of Information Systems

As noted above, the value of an information system does not lie in the sum of its categories or the volume of information collected, but rather in the ability to connect them to generate useful information and analysis that address the system's objectives. Thus, relational logic transforms a record of events into a useful tool for prevention, protection, investigation, reparation, and non-repetition. In this regard, the decisions made during data processing and the resulting outcomes will be decisive in enabling the system to move beyond the role of a passive event log and become an active infrastructure for guaranteeing the right to defend rights.

However, the type of processing possible and the resulting *outputs* will be shaped, to a large extent, by decisions regarding the information system's architecture, taking into account institutional capacities, the reliability of the information, the elimination of biases, and national or institutional contexts.

The chapter on information systems emphasized the value of moving beyond systems that merely compile existing databases toward one that allows for greater integration of information. This is because integrated systems can enhance learning and outcomes, enabling information to play a preventive and protective role and to strengthen individual and collective responses aimed at eliminating or mitigating risks and potential harm.

The comparative study of information systems and databases has identified limitations—whether legal, factual, or stemming from privacy or security

requirements—that hinder the sharing of various types of data, including demographic data, event data, or information related to ongoing legal proceedings or investigations. Some of the challenges posed by these limitations can be addressed through legally established guidelines on access, restricted use, or system of interoperability, taking into account contextual considerations and legal mandates. The fact is that the existence of multiple sources of information and databases related to attacks against human rights defenders is a reality, not an obstacle to overcome. In addition to information and databases from the administration of justice, there are those from autonomous entities within the State, thematic or subnational registries, and databases related to compliance with obligations toward environmental defenders under the Escazú Agreement, among others. Beyond these efforts, other fundamental initiatives from civil society—non-governmental organizations, universities, and think tanks—aim to document and analyze various aspects of attacks against human rights defenders.

Civil society databases were, in many cases, pioneering and contained valuable, sensitive, and timely information that was not documented by state or intergovernmental sources. Thus, they were early to document cases of surveillance, monitoring, enforced disappearance, or impunity targeting human rights defenders or particularly affected groups, such as women human rights defenders, environmental defenders, or people in exile. In adverse contexts—where key state actors responsible for protection, such as security forces or the justice system, are compromised or viewed with distrust—it has been civil society spaces—organizations, churches, and academic research centers—and international organizations that have offered the greatest guarantees of impartiality, confidentiality, and safety to those who speak out. This has led to robust systems that have access to information distinct from that processed by state entities, such as those of the Somos Defensores Program[75]; the Foundation for Press Freedom (FLIP)[76], Justiça Global[77],

75 Somos Defensores Program. *Information System on Attacks Against Human Rights Defenders in Colombia (SIADDHH)*. Available at: https://somosdefensores.org/siaddhh/

76 Foundation for Press Freedom (FLIP). *Murdered Journalists*. Available at: https://flip.org.co/cifras/periodistas-asesinados

77 Justiça Global. *Protection of Human Rights and Democracy Defenders*. Available at: https://www.global.org.br/es/blog/programa/proteccion-de-defensoras-es-de-derechos-humanos-y-de-la-democracia/

Global Witness[78], CIVICUS[79], the Unit for the Protection of Human Rights Defenders in Guatemala (UDEFEGUA)[80], and the Mesoamerican Initiative of Women Human Rights Defenders (IM-Defensoras)[81], among many others. Additionally, international bodies—such as the United Nations and the human rights protection mechanisms established by the OAS, among others—have produced valuable reports at both national and thematic levels. Among these, it is worth highlighting the work of the United Nations Special Rapporteur on the Situation of Human Rights Defenders, the Office of the United Nations High Commissioner for Human Rights (OHCHR), the Special Rapporteur on Freedom of Expression (RELE) of the IACHR, and the Working Group on Enforced or Involuntary Disappearances.

Therefore, it is necessary to consider how to fulfill the international mandate to ensure a state-run information system on human rights defenders that integrates—or can benefit from—the databases maintained by various entities, as well as complementary information that may emerge from other sources, in order to generate useful information for public policies and practices at different levels. This is necessary whether the goal is to better understand individual and collective phenomena in order to protect individuals, groups, and communities; to refine criminal policy decisions by taking into account relevant factors or potential predictors of lethal violence; or to guide processes for regulating hate speech or digital threats, among many other objectives.

Furthermore, given the patterns of violence in the region and the importance of civil society spaces—including academic ones—for the study of some of these phenomena, it is important that the redesign of information systems take these actors into special consideration. This approach involves not viewing government institutions as the sole relevant factor in shaping public policy and prevention practices but rather considering academia and civil society as fundamental actors in refining the State's own information analysis and actions to defend rights. Furthermore, doing

---

78 Global Witness. *Latin America and the Caribbean*. Available at: https://globalwitness.org/en/regions/latin-america-and-the-caribbean/?page=2#listing

79 CIVICUS (2024). *Violence Targets Journalists and Human Rights Defenders Without End*. Available at: https://monitor.civicus.org/

80 Unit for the Protection of Human Rights Defenders - Guatemala (UDEFEGUA). *UDEFEGUA*. Available at: https://udefegua.org.gt/

81 Mesoamerican Initiative of Women Human Rights Defenders (IM-Defensoras). *IM-Defensoras*. Available at: https://im-defensoras.org/

so allows us to recognize their immense contribution to democracy, civic space, and enjoyment of rights within the regional context and to foster positive synergies with these spaces. For example, by making information available in a way that facilitates access, as well as by creating interfaces that allow independent entities to contribute to parts of the system, with the aim of expanding access to rights, addressing biases, tackling silenced issues or areas, facilitating access to protection tools, developing self-protection measures, or supporting memorialization.

That said, the guidelines provided by international law for the development of national information systems in this area make it possible to outline minimum requirements and relevant outcomes for data processing. Thus, the Inter-American Court of Human Rights has held in various judgments that it is necessary to have a national information system on violence against human rights defenders[82]. The high court does not require a census of human rights defenders, based on the definition adopted by the Court itself[83]. Far from that, the Court requires that information be generated in accordance with the aforementioned categories and parameters, disaggregated at the subnational or state level, in order to produce statistics and information on patterns, events, and enabling contexts relevant to the exercise of the rights of human rights defenders—individuals, groups, and organizations— on the scale of the violence they face, as well as on the root causes of the attacks, and the preparation of at least one annual public report[84]. The objective of processing the collected information is to inform public policies and practices aimed at preventing and eradicating violence and to support an enabling environment for the exercise of rights[85].

The guidelines established by the court have implications for the type of data processing required and for the results or *outputs*. At its most basic level, this processing enables the production of disaggregated statistical information—for example, numbers and percentages of threats, displacements, or types of violations associated with certain demographic characteristics, as well as prevalence and trends by geographic area or time period—. However, understanding the scope and magnitude of the phenomena affecting human rights defenders in a timely and appropriate

82 See section 4 of the document.

83 See section 6.a. of the document

84 See sections 4 and 6 of the document.

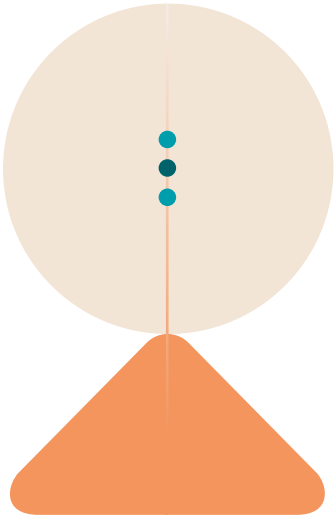
85 See sections 4 and 6 of the document.

manner—with a view to preventing harm—requires a certain capacity to link information and channel it to the various levels of the state apparatus for the purposes of protection, prevention, and investigation.

More complex analysis can draw on statistics and data science. Through various techniques—such as variable association, identifying which factors most influence the occurrence of an event, clustering, identifying patterns, or projecting risk scenarios, among others—it is possible to generate insights that are not apparent in the data when viewed in isolation[86].

The following section outlines some of the possible results or *outputs* of an information system on attacks against human rights defenders that could contribute to positively influencing the protection of human rights advocacy work.

86 It should be noted, however, that the effective use of these techniques depends on having standardized historical databases, homogenized information, data quality standards, and sufficient metadata to determine the origin, scope, reliability, and date of the last update of the information



IX. Selection of Anticipated and Possible *Outputs*

From the processing described above and the guidelines established by Inter-American case law, a range of possible outputs emerges, of increasing complexity, that must be taken into account when developing the information system on human rights defenders.

Thus, the system's potential outputs can be organized progressively according to the level of information processing. The first level includes descriptive outputs, such as statistics, periodic reports, alerts, and briefings. A second level incorporates visualization and synthesis tools, such as indices, maps, geoportals, and dashboards, among others. A third, more advanced level explores analytical and predictive models, including regressions, classification models, and structured extraction using language models, among other possibilities. Not all of these require the same level of technical expertise, and they should be understood as a scalable repertoire rather than a closed list[87].

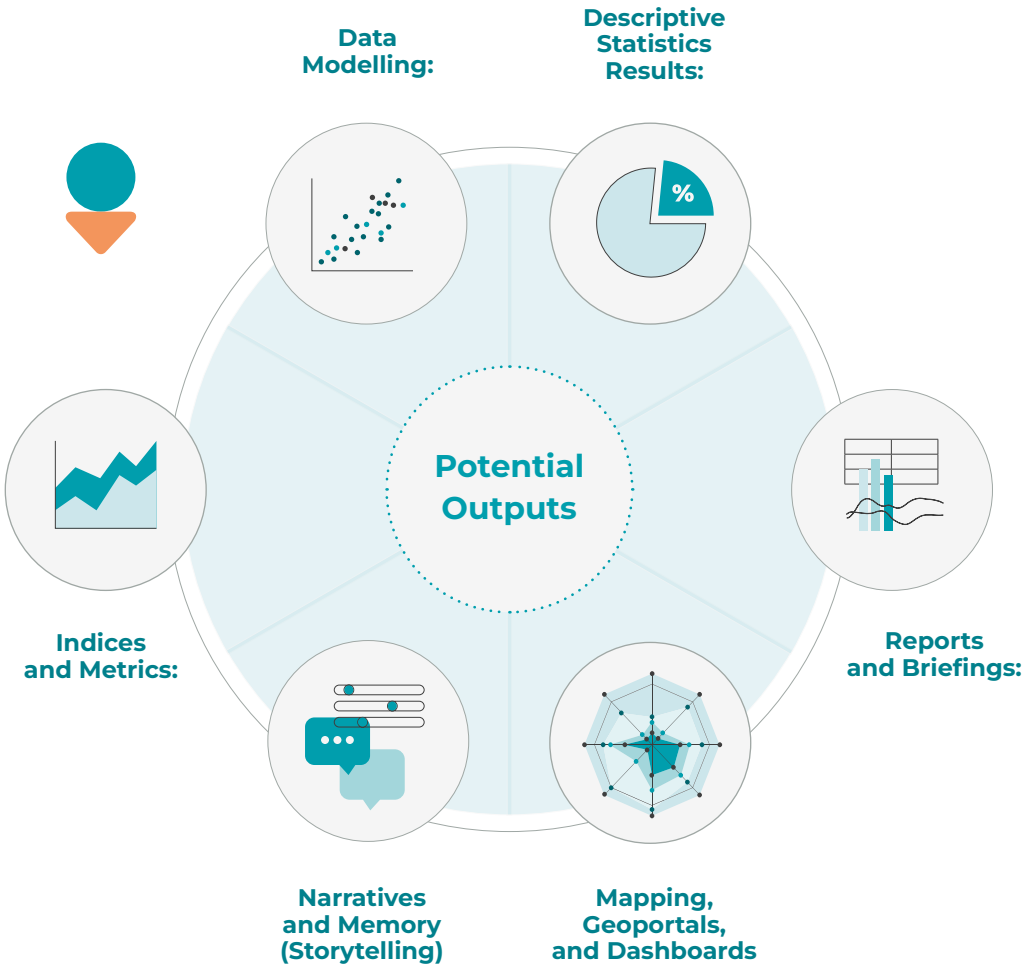
Each of the anticipated outcomes, even those at lower levels of processing, can lead to improvements in protection policies and practices. While we emphasize that progress in the levels of information processing is a key element of the system's

87 It should be noted that, while some of the results can and should be made public, others—or the information produced or its inputs—may be confidential, such as information relevant to individual protection measures or criminal investigations.

effectiveness, we note significant room for improvement in the development of *outputs*, as well as their integration with interfaces for the actions of various entities or organizations, as discussed later in the text.

This section first describes the main expected *outputs* of the information system on human rights defenders, then delves into two examples of predictive models, and concludes with guidelines for their responsible use.

Main Expected *Outputs*



a. Descriptive Statistics Results

The systematization of information allows for the generation of periodic and disaggregated statistics on various phenomena, which in turn make it possible to evaluate progress, setbacks, and milestones in the development of public policies. Some examples include the number of victims and incidents of victimization, as well as bivariate analysis by date, location, or alleged perpetrator. Other statistics of interest may include the percentage of the population affected, and a differentiated analysis based on variables such as gender or ethnicity, among others.

An important tool is the creation of time series, which allows us to see how incidents of violence evolve or how they relate to changes in policy, practices, or events over a given period (for example, quarterly, semiannually, annually, etc.).

It is worth noting that the Inter-American Court of Human Rights not only requires that statistics be available but also specifies certain categories and variables that must be collected in order to understand the various forms of aggression, their causes, their individual and collective impacts, and evolving trends.

b. Reports

The Inter-American Court of Human Rights specifies, as one of the required outcomes, an annual report on the subject and the State's responses. This report must comply with the principle of transparency and must explain matters such as the database(s) used, the processing of information, the models employed, and the conclusions drawn. Crucially, it must explicitly state the rationale behind methodological decisions and acknowledge any limitations. Additionally, to ensure access to information, this report should be available in different versions, ranging from technical and methodological language to plain language accessible to any citizen. Furthermore, participation mechanisms must be guaranteed to receive suggestions or criticism from the public, academic circles, or civil society.

At the same time, the preparation of quarterly reports, containing specific levels of detail, can serve to evaluate the phenomena and impacts of the measures, policies, and initiatives adopted in a more accurate and timely manner. In particular, the use of *dashboards*—which graphically display part of the report's information and allow for greater cross-analysis of variables and time periods—can be extremely useful for making the information in the required report more accessible and useful.

c. Mapping, Geoportals, and Dashboards

These information visualization tools facilitate the identification of patterns, trends, risk factors, actors involved and areas of particular vulnerability over time, and contribute to the design of institutional prevention, protection, and response measures. The true analytical power of these platforms lies in their ability to overlay different layers of information simultaneously. An isolated analysis offers a limited view, but combining multiple factors can reveal hidden dynamics. For example, simultaneously visualizing deforestation levels (a pattern variable) alongside threats (an aggression variable) can highlight a possible correlation between the two phenomena.

These tools must be accessible to the general public. That is, they must be accompanied by clear manuals, intuitive tutorials, and data dictionaries that explain the variables presented along with their respective documentation methodologies. Furthermore, they must feature a user-centered design, allowing non-technical users to navigate and understand them.

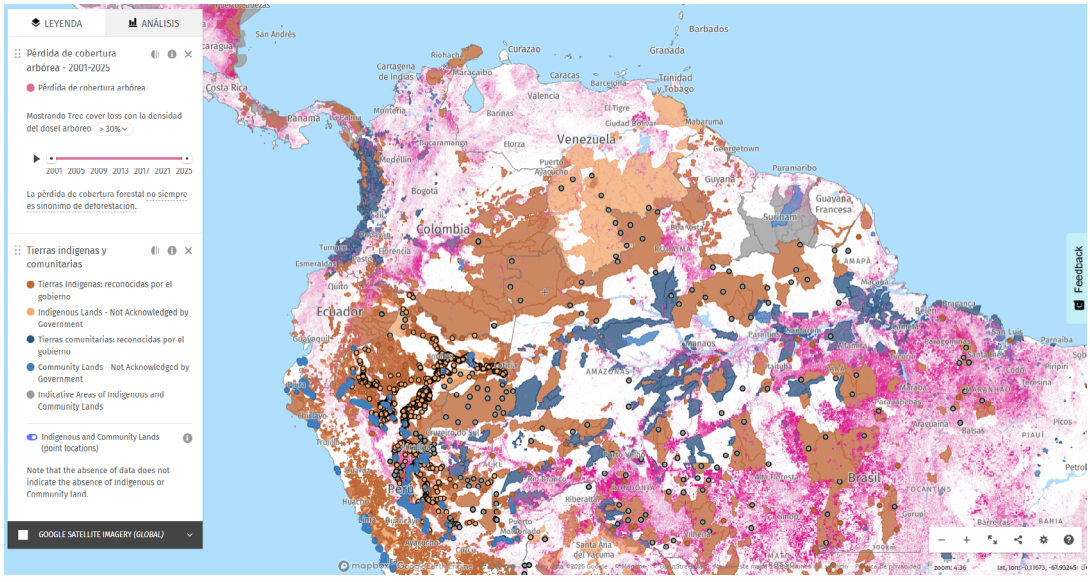
As an example, the following image shows a visualization dashboard from Armed Conflict Location & Event Data (ACLED). In the left panel, the user can select different countries to compare conflict levels across its four indicators. This makes it possible to visualize the strengths and weaknesses of multiple countries and make visual comparisons. Meanwhile, in the right-hand panel, users can compare the rankings of the indicators for all countries or for specific ones.

ACLED Conflict Index Rankings

Country	Index Level	Total Rank	Deadliness Rank	Diffusion Rank	Danger Rank	Fragment... Rank
Palestine	Extreme	1	3	1	1	9
Myanmar	Extreme	2	4	8	6	1
Syria	Extreme	3	7	4	5	8
Mexico	Extreme	4	8	16	2	3
Nigeria	Extreme	5	5	16	7	10
Ecuador	Extreme	6	15	11	8	12
Brazil	Extreme	7	9	30	4	4
Sudan	Extreme	8	2	26	10	15
Haiti	Extreme	8	14	6	20	13
Pakistan	Extreme	10	13	20	13	11
Ukraine	High	11	1	5	3	51
Democrati...	High	11	10	29	15	6
Cameroon	High	11	22	12	9	17
Colombia	High	14	19	24	14	5
Yemen	High	15	18	10	16	25
India	High	16	23	42	11	2
Somalia	High	17	6	13	19	46
Guatemala	High	17	28	14	23	19
Russia	High	19	20	34	12	25
Lebanon	High	19	35	2	30	24

Source: ACLED (n.d.) Conflict Index Dashboard. Retrieved from: https://acleddata.com/platform/conflict-index-dashboard (June 24, 2026).

Additionally, the following image shows an example of a Global Forest Watch geo-portal. Here, users can select multiple layers to view, such as tree cover, soybean plantations, mining concessions, or indigenous and community territories. This allows users to overlay different layers and conduct visual analyses. The example shows a map of South America with two layers activated: tree cover loss (2001–2025) and indigenous and community territories, allowing users to visually identify areas where both phenomena coexist geographically.



Source: Global Forest Watch (n.d.) Map. Retrieved from: https://www.globalforestwatch.org/ (June 24, 2026).

d. Narratives and Memory (Storytelling)

These systems can also give rise to products focused on individual stories and memory. In this regard, some of the initiatives led by civil society have been pioneers in documenting and telling these stories through testimonial accounts, profiles and biographies of human rights defenders, memory maps, digital galleries and memorials, and platforms for raising awareness, among others[88].

These formats can be integrated into the system; for example, through *storymaps* dedicated to human rights defenders (WHRDs) and organizations, which recount their history, career paths, and contributions, so that end users can learn about and recognize their work and strengthen their visibility. In this way, these products combine the documentary function of the registry with its dimension of memory and reparation[89].

e. Indices

Indices are analytical tools that synthesize multiple variables—for example, the frequency of attacks, the level of impunity, and the presence of armed actors—into a single standardized metric that is comparable across regions or time periods.

In an information system on human rights defenders, indices provide benchmark metrics that allow for comparing the state of the situation across different regions, constructing rankings, and, on that basis, prioritizing early warnings and guiding advocacy actions according to the severity of the detected risk. Their construction can combine structural and territorial variables (such as the presence of armed

---

88 See, for example, the narrative and memorialization series from the Somos Defensores Program, available at https://somosdefensores.org

89 Below are some examples of memorialization efforts. Regarding those executed in Iran, the *Omid Memorial* at the Abdorrahman Boroumand Center documents and tells the stories of those who were arbitrarily deprived of their lives (available at https://www.iranrights.org/memorial). In the field of journalism, the exhibition "(Im)possible Forms of Journalism: A Profession in the Midst of Conflict," part of FLIP's *"Memories of Journalism in Colombia"* project, offers a journey through the profession's past (available at https://memoriasdelperiodismo.co/periodismos-posibles/). Regarding missing persons, systems have been created in Mexico to support investigations, find clues, and identify and locate victims, such as the *Angelus* system of the National Search Commission (available at https://seguridad.conahcyt.mx/guerra-sucia/angelus) and the Public Inquiry of the National Registry of Missing and Unlocated Persons (RNPDNO) (available at https://consultapublicarnpdno.segob.gob.mx).

groups, illicit economies, illegal mining, displacement, and illicit crops, among others), so that a complex phenomenon can be expressed in values that facilitate the identification of patterns, comparison, and tracking of trends. Furthermore, they allow for the integration of multiple sources of information on a single issue, making it possible to recognize its variability. They can even incorporate indices from other entities or organizations to enrich the analysis when primary data is unavailable.

These indices can be integrated into data visualization or modeling tools to reveal hidden correlations, test hypotheses, or project future risk scenarios.

For example, the ACLED conflict index presented above is based on four dimensions: fatalities, danger, geographic spread, and fragmentation of armed groups.

f. Modeling

One approach within the information system involves using statistical and machine learning tools to transform data into evidence that informs decision-making. This can be particularly useful when dealing with vast amounts of information, but also for explaining and resolving underreporting issues. Model applications can serve various purposes, as outlined below.

It is important to note that models do not require only structured data—that is, data that can be organized into rows and columns. It is possible to use unstructured data, such as audio, video, and text, to generate outputs like those presented in this subsection.

Furthermore, it is worth emphasizing that the most advanced analytical capabilities of statistical or *machine learning* models do not replace institutional judgment or human intervention. As indicated in the governance guidelines of this document, no decision regarding protective measures should be made based solely on an algorithm. However, these models can be valuable tools for prioritizing assistance, detecting early warning signs that might be missed during manual review, and directing the allocation of institutional resources toward the individuals, groups, and areas at greatest risk, among other functions.

At the level of document management, machine learning models are essential for deduplicating records, ensuring that the same incident or victim is not counted redundantly. Once a consolidated database is established, this information facilitates

the study of documentation patterns specific to each source. The above helps in understanding the strengths and weaknesses of diverse sources, as well as in identifying potential biases or gaps.

In the field of causal analysis, these tools can measure the impact of different variables on a situation of vulnerability. The system can process multiple factors simultaneously to determine which of them has the most decisive influence on a key variable of interest, such as fluctuations in risk levels.

Likewise, through hypothesis testing, it is possible to statistically verify how a single phenomenon affects different populations or geographic areas unequally, providing evidence to justify differentiated protection approaches.

Meanwhile, the implementation of automatic *clustering* models allows for the grouping of victims or incidents based strictly on their intrinsic similarities, without the need to impose predefined categories. This helps reveal shared behavioral patterns and underlying dynamics that serve as essential resources for anticipating risk scenarios, optimizing resource allocation, and substantially improving the design of prevention policies. Undoubtedly, these models can make significant contributions to a public policy approach with a macro-criminal perspective, as well as to a protection policy that refines the criteria for addressing various vulnerability factors. Additionally, the system can integrate predictive models that transform historical and contextual analysis into forward-looking intelligence. By processing the past behavior of variables, these algorithms are designed to calculate the probability of future incidents occurring in the short or medium term, or to identify escalation patterns that, if not addressed in a timely manner, lead to serious and irreversible harm to human rights defenders.

Below are two simple examples of possible uses of models with both structured and unstructured data, illustrating potential applications of information systems for prevention.

i. Predictive Model Using Structured Data

There are numerous predictive models that can be used to support decision-making and protect human rights defenders. While the objective of *this blueprint* is not to cover every possible method, this section briefly introduces logistic regression using a hypothetical example that seeks to predict the probability of a human

rights defender being killed based on previous threats and other individual characteristics[90] .

Logistic regression is a standard statistical method in the field of machine learning, specifically designed to predict binary outcomes—that is, situations where there are only two possible outcomes. For example, determining whether a human rights defender is at risk of being killed or not.

The model works by estimating a probability ranging from 0 to 1 for each individual, basing its calculation on a rigorous analysis of their observable characteristics at the individual level. For this process to be possible, the algorithm must be fed a dataset structured at the individual level, where each record or row corresponds to detailed information about a human rights defender, covering both the variable of interest or dependent variable ("killed" vs. "not killed") and a series of independent variables that reflect their characteristics, such as gender, ethnicity, the type of leadership they exercise, the geographic area, or a history of previous attacks.

The central objective of this algorithm is to process historical information to learn how to identify and quantify the relationships between the various characteristics and the fatal outcome. During this training phase, the model evaluates past data and assigns a specific mathematical weight to each variable, which reflects how strong or decisive its association with the final outcome is. Once the system has consolidated this knowledge and defined the weights using a mathematical formula, it is capable of processing completely new and unknown information. Thus, when the government or an organization enters data on defenders whose current level of danger is unknown, the model is able to project the probability of risk based exclusively on the patterns it has previously learned.

90 This section draws on the work carried out by GRIL, which developed a logistic regression prototype based on synthetic data with the aim of introducing a predictive model to a non-technical audience. The model was built using aggregated statistics from public reports—such as the Semiannual Reports of the Somos Defensores Program and the Electoral Observation Mission's report on violence against community leaders. The model estimated the probability of assassination based on variables such as the type of advocacy work, ethnicity, gender, and the history of previous attacks. Using a dataset of 5,000 simulated records and a split between training data (80%) and test data (20%), the model achieved an area under the ROC curve of 0.89, indicating a high ability to distinguish between higher- and lower-risk cases. The factor with the greatest predictive power was the existence of documented prior attacks, followed by the type of advocacy work.

The use of logistic regression is very common in the initial phase of predictive projects because it offers clear operational advantages over other, more complex methods, standing out primarily for being a relatively easy-to-interpret model. Its analytical transparency allows decision-makers to accurately identify which specific characteristics are linked to the highest risk levels, since those variables will be directly reflected by the highest numerical weights in the formula.

Furthermore, it has the merit of translating historical patterns into quantifiable and comparable estimates, which can guide the prioritization of cases within protective measures or the prioritization of criminal investigations. In this way, the example presented here enables considerable progress in key measures to prevent fatal injuries.

That said, these models—which represent significant advances over the current situation in most contexts—have limitations that can be overcome by other tools. Thus, they present a structural limitation relevant to the purposes of this system: they reduce the complexity of violence against human rights defenders to a single variable of interest (in this case, a binary outcome of homicide), ignoring the broad spectrum of violations that precede, accompany, or replace homicide. For example, arbitrary detention, forced displacement, community confinement, the risk of recruitment of children and adolescents, and gender-based violence in contexts of armed conflict. All of these are documented and foreseeable outcomes that a model focused exclusively on death does not capture.

Therefore, it is possible to use more complex models that allow for the identification of multiple risk variables. This is because an information system on human rights defenders must be geared toward prevention, which requires identifying violations before they escalate into the most serious forms of attack.

ii. Large Language Model with Unstructured Information

Natural language models are useful for analyzing qualitative information presented in texts. Specifically, in this example, it was used to extract structured information (which can be organized into a table) from unstructured documents. This capability is particularly relevant for the information system on human rights defenders, given that a substantial portion of the available information is found in narrative reports, early warnings, records from civil society organizations, and institutional reports that are not systematized in databases.

In the example discussed in this section, a natural language processing model for unstructured data was used, based on early warnings from the Colombian Ombudsperson's Office. This made it possible to test a model that links a greater number of events and variables to gain better insights into potential escalations of violence, consequences for different individuals, and institutional response times. The model is not intended to evaluate institutional responses to the specific events included in the example; however, it could be refined to analyze certain patterns affecting human rights defenders and their communities, real-time variations in these patterns—such as escalations and effects on various groups—the impacts of institutional interventions by different entities, or the actions of other actors.

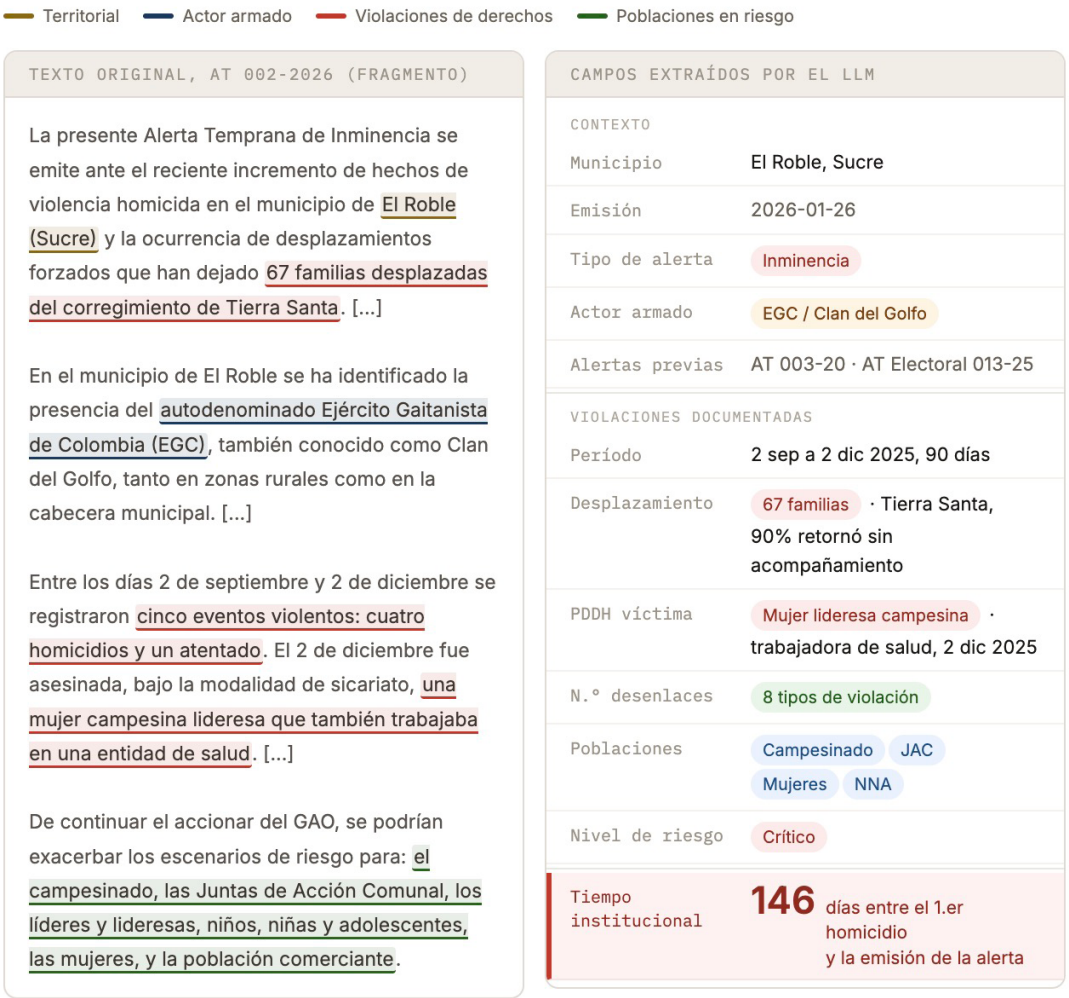
In turn, the results of this structured extraction serve as input for more sophisticated causal analysis, *clustering*, and risk estimation models, as described in the previous sections of this chapter. The rationale for their use is cumulative: the quality of the analysis depends on the quality of the available structured information, and automatic extraction using language models allows this structuring to be scaled to volumes of information that could not be processed manually.

As an example, consider the Early Warnings of Imminent Danger issued by the Colombian Ombudsperson's Office[91]. These warnings, which can be downloaded from the public portal of the Early Warning System (SAT), are documents ranging from 10 to 20 pages that describe the territorial context, the background of the risk, recent violent incidents, the affected populations, and recommendations to the relevant institutions. Their content is narrative and heterogeneous, which makes it difficult to integrate them directly into structured databases.

Using a language model, it is possible to automatically transform the text of these alerts into a set of structured fields: the chronological sequence of violent events with their dates and types, the identified armed groups and documented actions, populations at differential risk—including human rights defenders—indicators of conflict escalation, and the gap between the first recorded events and the institutional response. This extraction process can be systematically applied to hundreds of alerts, generating an analytical database that allows for the study of patterns over time and across the territory.

91 For more information, see: https://alertastempranas.defensoria.gov.co/

To illustrate this capability, we specifically examined Early Warning No. 002-2026 on Imminent Threat, issued by the Ombudsperson's Office on January 26, 2026, for the municipality of El Roble, Sucre. From the text of this single document, the model identified eight distinct types of rights violations, five indicators of escalation, six populations at differential risk, and a 90-day timeline leading up to the murder of a female leader. The following figure shows this extraction: on the left, the original text of the alert with the relevant passages underlined; on the right, the structured fields that the model derives from them.



Source: Early Warning No. 002-2026 on Imminent Threat, Colombian Ombudsperson's Office, January 26, 2026. Automated structured extraction using a language model

One of the analyses enabled by the tool was the identification of an escalation pattern. Thus, between September 2 and December 2, 2025, the municipality recorded five violent incidents over a ninety-day period: a first homicide in El Sitio; a double homicide in Tierra Santa committed by a group of between eight and ten uniformed men without insignia—an atypical modus operandi that led to the

hypothesis of a possible second armed group—; an attack resulting in a serious injury in Tierra Santa; a homicide in the municipal seat—marking the spread of violence into the urban area—; and, finally, the murder of a female peasant leader who also worked as a health care provider in the village of El Sitio. This sequence, which is not immediately recognizable as a pattern in a record of isolated events, becomes analytically legible as a trajectory of escalation: a rupture in the apparent calm, a change in modus operandi, geographic expansion, and one of the outcomes involves a human rights defender as a victim.

This sequence is illustrated in the following image, which shows how the events, viewed over time, form a pattern of escalation.

Source: Early Warning No. 002-2026 on Imminent Threat, Colombian Ombudsperson's Office, January 26, 2026. Automated structured extraction using a language model

The model also identified five indicators of escalation[92] and determined eight adverse impacts: the murder of the female leader; the forced displacement of 67 families from the District of Tierra Santa; the return of approximately 90% of the displaced families without institutional support; collective threats against those who reported to the authorities; systematic extortion of officials and merchants; pressure on Community Action Boards to act under the armed group's directives; the risk of recruitment and use of children and adolescents in micro trafficking activities; and the risks of gender-based violence in the context of armed control.

Additionally, it made it possible to measure institutional response times: the model calculated a period of 146 days (about 5 months) between the first documented lethal event (September 2, 2025) and the issuance of the alert (January 26, 2026). This data is analytically relevant: it documents the time elapsed between the warning signal and the formal response from the alert system and can be studied comparatively across the entire corpus of alerts or in relation to other interfaces with rights protection systems. In this case, the methodology was applied to alerts, but it could be expanded to include other types of data from individual and collective protection systems, public safety measures, etc.

When systematically applied to the entire set of Early Imminence Alerts available on the Ombudsperson's public portal[93], this methodology would allow for the creation of a structured database containing information on escalation trajectories, patterns of action by armed groups, the territorial distribution of results, the gap between events and various institutional responses, and differential risk patterns for human rights defenders. This corpus could be enriched with alerts from civil society organizations or supplemented with protection measures arising from civil society processes.

---

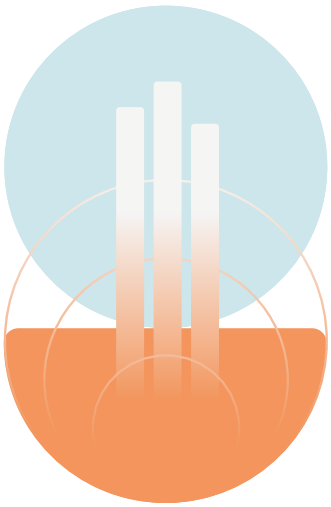
92 Namely: (i) a prolonged absence of lethal violence in the preceding eight months—which the Ombudsperson's Office interprets as a consolidation of the armed group's hegemonic control, not as peace—; (ii) an abrupt break in the pattern with five incidents in ninety days; (iii) a change in modus operandi; (iv) a shift from rural areas toward the municipal seat; and (v) the murder of a human rights defender as the culmination of the sequence.

93 As of the date of this document's preparation, more than 350 alerts have been issued between 2017 and 2026. For more information, see: https://alertastempranas.defensoria.gov.co/

g. Considerations for Responsible Use

The application of models in the context of information systems on human rights defenders requires specific safeguards, although some of these also apply to the development of indices and other information processing systems. First, the results of the models must be treated as inputs for institutional judgment and not as autonomous determinations: the *outputs* of the models—risk estimates, pattern identification, and gap calculations—must be verified and contextualized by human teams with territorial and legal expertise. Second, the data extraction methodology and classification criteria used must be transparently documented and made available for review, so that the results are auditable and reproducible. Third, it is important to remember that statistical algorithms simplify reality and can perpetuate biases present in historical data, which may end up revictimizing or excluding vulnerable populations. Finally, any large-scale implementation must undergo a risk analysis that assesses potential misuse of the consolidated information, in line with the principles of "do no harm" and "legitimate use" outlined in the chapter on ethical principles in this document.

With these safeguards in place, the analytical models described in this section represent a significant advance over existing descriptive approaches: they not only document what happened, but also reveal what was happening before it occurred, and they do so with the systematic rigor necessary to guide evidence-based institutional responses.



X. Institutional and Civil Society Interfaces

The system's outputs must be designed to integrate with interfaces that ensure real impact on prevention, protection, investigation, and public policy formulation. International law is very clear in defining obligations of response and due diligence regarding foreseeable and known risks, which translate into obligations to produce information, disseminate it, and take action by various state entities with authority over the matter.

However, it is not enough to simply produce reports, maps, alerts, indices, or models: these must be able to reach—with the appropriate level of detail—the authorities responsible for adopting measures, activating protection pathways, prioritizing territories, or strengthening investigations. To this end, the system should include distinct interfaces for government entities, including alerts focused on protection and prevention, mechanisms for territorial targeting, and specific products for investigative bodies and the administration of justice, as well as for disseminating information appropriately and in a timely manner to individuals or groups at risk.

These interfaces must be designed with interoperability standards that allow for their integration with the information systems of the competent and relevant entities at the national or local level to address the issue. For example, entities such as the Attorney General's Office, the National Protection Unit, or mechanisms for the protection of journalists; the Ombudsperson's Office or national human rights institutions; the Ministry of the Interior, security, or justice; or other institutions with functions related to prevention, protection, investigation, or prosecution. To this

end, standardized data structures, common metadata, secure exchange protocols, differentiated access rules, mechanisms for tracking the use of information, and guidelines for its appropriate and timely distribution or dissemination to relevant entities, organizations, or international bodies must be considered[94].

Given the realities and characteristics of data collection in this area, the State's information system on human rights defenders must include interfaces with civil society organizations. This can be particularly useful for cross-checking and analyzing data, eliminating biases, and advancing public policy objectives through synergies with other non-state information systems and mechanisms for safeguarding rights. On our continent and globally, civil society organizations, academia, and specialized institutions play a substantive role in documenting, verifying, and making information publicly available, as well as in providing legal, psychosocial, medical, and humanitarian assistance services, among others. Their work makes it possible to support at-risk individuals and communities, launch advocacy initiatives, strengthen independent monitoring, contribute to upholding the rule of law, support measures for the protection and self-protection of individuals and communities, and disseminate key information in a timely and appropriate manner, among other things. Therefore, the state information system on human rights defenders must provide for possible coordination with data from non-governmental sources in order to strengthen the data collected and the analysis produced—as well as forms of public or semi-public access to results—, through differentiated levels that allow the information to be utilized without compromising the security of human rights defenders, victims, witnesses, communities, sources, or security policies and criminal investigations. In addition, there should be provisions for specific active transparency products regarding institutional performance—statistics, reports, and others mentioned above—that can open the door to interfaces and synergies with civil society and academic spaces at the local, national, regional, and global levels.

Below, we list some of the possible interfaces that could be useful for information systems on attacks against human rights defenders that support prevention, protection, investigation, accountability, and reparations. These include: i) interfaces for individual prioritization, ii) alerts regarding groups at risk, iii) interfaces with the

94 DANE – SEN. *Recommendations on mechanisms, standards, and protocols for interoperability in the exchange, use, and reuse of data in the SEN*, May 2025, dimension 4, pp. 39–40.

administration of justice and investigative bodies, and iv) interfaces with spaces dedicated to the protection of rights and memory.

a. Individual Prioritization Interfaces

These interfaces may include communication channels and individualized responses, with differentiated levels of information and access for the various competent entities. Their purpose is to facilitate a coordinated response to situations of individual or collective risk in an appropriate, timely, and—where applicable—consensual manner. The definition of these interfaces will depend on the institutional pathways that each State establishes to respond to an identified risk based on individualized findings affecting a person or groups of people.

As noted above, the channels and interfaces must include a validation process carried out by individuals with the technical expertise and contextual knowledge necessary to interpret the results and define the most appropriate response measures across the various institutional spheres. These may include agreed-upon protective measures, enhanced investigative measures in response to associated threats or events, family, medical, or psychological support measures, if necessary, police security measures, and other relevant actions depending on the characteristics of the case.

An example of this type of information system, based on targeted data use, is the platform developed by Impulso.gov for Brazil's Unified Health System[95]. It combines data, evidence-based models, and differentiated access levels to guide preventive actions by community health teams through micro-targeting strategies, coordinating the efforts of public entities and health workers in the communities. What is particularly interesting about this initiative is its approach to differentiated information management and access levels, which enables timely responses from the relevant institutions.

b. Alert Interfaces for At-Risk Groups

International obligations related to addressing certain or imminent risks apply to both affected individuals and groups. Within this framework, due diligence

95 For more information, see: https://www.impulsogov.org

obligations entail taking adequate and timely measures to inform potentially affected individuals or groups of such risks, as well as implementing appropriate actions to mitigate them.

The collective dimension of human rights advocacy is not always adequately documented or addressed. This is due, in part, to the fact that specialized literature and public policy have tended to prioritize the analysis of individual attacks and fatal incidents. However, many attacks against human rights defenders seek to silence, slow down, or inhibit collective human rights advocacy efforts. In fact, much of the advocacy work has a collective dimension, both in terms of how rights defense processes are organized and in terms of the rights, communities, and individuals involved. For example, members of a non-governmental organization defending an indigenous community against a criminal organization encroaching on a specific territorial area.

The timely and adequate dissemination of information on situations of risk constitutes, in and of itself, a measure of prevention and protection. The State has a duty to proactively collect and disseminate information on situations of risk in a comprehensive, clear, truthful, up-to-date, and timely manner, through accessible channels and in language understandable to different sectors of the population[96]. Consequently, the system must include distinct rules and workflows to warn the affected individuals, organizations, and communities—in a timely manner and in an appropriate format—about identified risks, so that they can make informed decisions regarding prevention and self-protection.

Likewise, these interfaces can facilitate prevention and self-protection measures driven by civil society. In many contexts, civil society networks and organizations have their own monitoring, alert, and response mechanisms—both individual and collective—and operate as channels for the timely and appropriate dissemination of information in local areas and communities. Therefore, the system interfaces should provide differentiated access options and feedback mechanisms that allow these actors both to receive relevant alerts and to contribute relevant information to strengthen community self-protection strategies.

---

96 Inter-American Court of *Human Rights. Advisory Opinion OC-32/25 "Climate Emergency and Human Rights,"* paras. 488–489, 503–504, and 521–523; CEJIL. *Access to Climate Information and Human Rights Obligations. Thematic Guide for Analyzing Advisory Opinion OC-32/25*, January 2026, pp. 5 and 13–14.

In this vein, developing interfaces that make these dynamics visible can be important—not only to highlight collective acts of intimidation, stigmatization, theft, and other forms of aggression, but also to document the protection and self-protection mechanisms promoted by civil society as strategies to prevent future crimes against social groups that defend rights (for example, demarcating boundaries, providing safe houses, strengthening community patrols, among others). Recording these actions would also make it possible to compare prevention efforts driven by citizens with existing public policies, highlighting the need to move toward protection models with a greater emphasis on collective and preventive dimensions. Similarly, collective measures implemented through civil society protection funds can offer valuable insights into the incorporation of intersectional approaches, with the aim of reducing the risks faced by communities and the human rights defenders within them.

c. Interfaces for the Administration of Justice and Investigative Bodies

The information system on human rights defenders should include a specialized interface for investigative and judicial bodies, designed to strengthen the identification, investigation, and prosecution of attacks against human rights defenders. As noted above, the results provided by some of the tools within an information system can help to better understand criminal networks and the sequences of crimes, identify individuals, areas, and groups at risk, and do the same with regard to alleged perpetrators. Additionally, it is possible to model and better understand the consequences and costs of the lack of timely intervention by state entities responsible for protection, as well as the effects of impunity.

Given the sensitive nature of some of this information and the need to preserve the integrity of investigations, access to individual data and procedural details must be governed by strict information security protocols, controlled access, and traceability of queries, with special confidentiality regarding the identities of witnesses and sources.

One of the areas where an information system can contribute is to the investigation of homicides and related crimes that are linked to various forms of violence, including lethal violence.

More disaggregated information on murder victims, perpetrators, and networks associated with crime—from a macro-criminal perspective—along with tools that allow for linking other data and crimes to the rise in lethal violence, can serve to

strengthen investigations, link cases, determine patterns, identify potential connections based on related variables, and prioritize certain crimes. Thus, for example, some of the models used above and the experience of the community studying violence against human rights defenders demonstrate the importance of criminal prosecution of threats in solving and preventing homicides, understanding macro-criminal patterns, and linking various criminal networks.

Additionally, it is essential that entities involved in the administration of justice adopt a policy of active transparency on the platform, allowing for open or controlled access to critical information on the status of cases—procedural progress or setbacks, convictions, appeals, sentence enforcement, etc.—. This entails greater transparency and cooperation with civil society organizations and academia, as well as among the institutions themselves. Likewise, forums should be promoted to cross-check disputed data or criteria regarding the classification of individuals as human rights defenders. An interface that facilitates dialogue on these issues would also help bring light topics or areas that remain overlooked in the institutional information systems. For example, in Colombia, there are discrepancies and gaps in information regarding the murders of human rights defenders and the criminal proceedings related to investigating these cases, with varying data among state agencies, international organizations, civil society organizations, and academia.

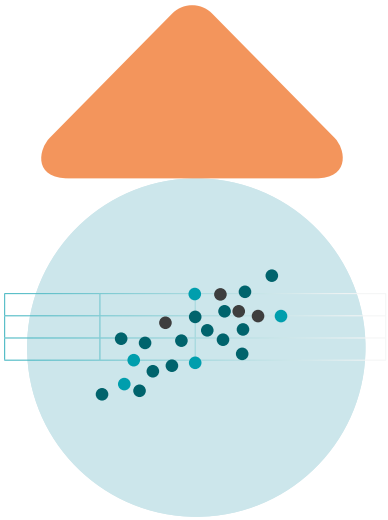
d. Interfaces with Spaces for the Protection of Rights and Memory

Civil society organizations, international organizations, ombudsperson offices, public defenders' offices, and truth mechanisms—such as truth commissions and transitional justice or memorialization processes—play a fundamental role in protecting the rights of human rights defenders and in building collective memory regarding the violence they face. The information system can coordinate with these entities to strengthen prevention, protection, investigation, and accountability.

The value of coordinating these entities lies in the fact that a risk or event detected by the system can be channeled toward an appropriate response, which is often multidimensional and exceeds the capacity of a single state institution. Thus, the information from the system can help guide and activate—depending on the needs of each case—legal support and representation for victims and groups, protective measures, psychological and psychosocial support, medical care, temporary relocation or shelter, and cultural and linguistic support—including adaptation to the languages of the affected peoples and communities. In turn, because of their

proximity to at-risk individuals and communities, these actors serve as a source of feedback for the system. To ensure that this coordination does not create new risks, the interfaces must provide restricted or controlled access for victims and their representatives, preserving the confidentiality and safety of those involved.

Furthermore, systematized information can be used and integrated with the advocacy efforts of victims and collectives—supporting strategic litigation, claims for reparations, and proceedings before national authorities and international protection bodies—as well as with truth and memory processes. In this latter context, the narrative products described above can inform truth commissions, archives, and memorialization processes. These interfaces must operate with the consent of the individuals and communities involved and under a victim-centered approach, so that memory strengthens—rather than compromises—their safety.



XI. Ethical Principles for the Design, Operation, and Use of Information Systems on Human Rights Defenders

Any information system, such as the one proposed here, regarding attacks against human rights defenders must be governed by rigorous ethical principles.

The first of these is the principle of *do no harm*. The collection, storage, or dissemination of data must never increase the risk to human rights defenders or expose their families, communities, sources, or affiliated organizations or processes. Risk mitigation measures, such as tracking access to sensitive information, must be central to the design and implementation of information systems.

Inseparably linked to this guiding principle are the principles of *legitimate use and precaution*. Likewise, each record must be guided by an explicit purpose that is proportionate and in accordance with inter-American standards. Furthermore, its design and operation must incorporate safeguards that prevent the collected information from being used for the purposes of persecution, surveillance, profiling, or stigmatization of human rights defenders, their families, the organizations to which they may belong, or the communities they serve. The guarantee of these principles is not merely declaratory; rather, it requires verifiable institutional mechanisms for internal and external oversight that enable the detection and correction of misuse of the system.

Additionally, it is imperative to consider the principles of *privacy*, *confidentiality*, and *digital security*. Information must be handled in accordance with the principles

of data minimization, restricted access where appropriate, and protection against misuse. Where applicable, there must be clear mechanisms for *informed consent* and for explaining the possible uses of the information collected.

The principles of *equality and non-discrimination* are also essential. The system must be capable of identifying differentiated impacts without reproducing structural biases or historical exclusions. One of its strengths may be to resolve or mitigate information gaps and biases in data collection.

Finally, *transparency*, *auditability,* and *effective protection of rights* must guide both the institutional design and the day-to-day operation of the system. The existence of active transparency obligations on the part of the State must ensure the production of information essential for policies protecting human rights defenders and for an enabling environment for the exercise of rights by all people. Additionally, these obligations extend to the system's institutional design and operation in order to guarantee scrutiny of the methodology used to produce information. In turn, the State's information system on human rights defenders must be oriented toward the effective protection of rights, reaffirming as the benchmark for measuring its value the effective capacity to guarantee the lives and rights of individuals, social leaders, organizations, and communities involved in the defense of rights.

XII. Guidelines for the Governance of the Information System

Governance addresses a question that precedes any technical decision: who manages the system, under what rules are decisions regarding its design and operation made, how are responsibilities distributed among the entities and actors that produce or coordinate the information, and how is it shared. In contexts characterized by a multiplicity of sources, governance is precisely the mechanism that enables the strategy of harmonization—rather than substitution—to be implemented, thereby ensuring the reliability of the information and its use for the protection of rights[97].

For governance to have practical effects, it must be embodied in a minimal institutional structure that determines who is involved, what functions they perform, how they use and share information, and under what oversight rules they operate. This structure may include, at a minimum: a technical coordinating body responsible for the system's operation and continuity; a technical-methodological committee responsible for decisions regarding variables, quality, and interoperability; an ethics, security, and data protection committee that oversees the handling of sensitive information; a permanent mechanism for the participation of human rights defenders,

97 For example, the mandate for coordinated implementation set forth in Ruling SU-546 of 2023 and Order 845 of 2024 of the Colombian Constitutional Court, which require coordination among multiple entities (Ministry of the Interior, Ministry of Defense, Ministry of Justice, Ministry of Finance, National Population Directorate, Office of the Attorney General, Office of the Ombudsperson, and Prosecutor's Office) under a unified conceptual framework and in accordance with the principles of habeas data.

communities, and civil society organizations, which intervenes at key moments in the system's life cycle—the design of categories, variables, access rules, and audits; the validation of risks and safeguards; the review of public products; and the periodic evaluation of their impact—; protocols for information exchange among entities that produce or coordinate data; differentiated access rules and traceability based on sensitivity levels; independent audits throughout the data lifecycle; accessible procedures for reporting misuse, with complaint and reparation mechanisms; and rules for suspending access in the event of risks, incidents, or data breaches.

This institutional architecture is consistent with the OAS's Inter-American Guidelines on Data Governance and Artificial Intelligence, which recommend establishing offices or entities with technical responsibility, precisely defining roles and responsibilities throughout the data lifecycle, and providing for multi-stakeholder participation mechanisms[98].

An information system on attacks against human rights defenders only fulfills its protective function if it incorporates mechanisms for the meaningful participation of the defenders themselves, the affected communities, and civil society organizations in its design, implementation, and evaluation. This requirement is not merely procedural: it directly addresses the deep mistrust that those who exercise the right to defend human rights have historically expressed toward the creation of state databases or registries—a mistrust fueled by a history of information being used for purposes of persecution, assassination, or profiling—. A significant challenge lies in defining how to integrate government data while taking into account civil society registries, without compromising the trust or security of the sources, preserving the autonomy of each registry, and ensuring that participation serves as a substantive check on the legitimate uses of the system.

Defining roles and access profiles requires specific attention, given their importance for security, traceability, and the legitimate use of information. In this regard, it is important to explicitly distinguish between permissions for recording, viewing, and managing information, taking into account both the sensitivity level of the data and the needs of each type of user. This distinction serves a dual purpose: it protects the information of human rights defenders, victims, witnesses, and sources, and

98 OAS. *Inter-American Guidelines on Data Governance and Artificial Intelligence*, 2024, available at: https://www.oas.org/ext/es/democracia/publicaciones/program/127

it strengthens the trust of those who contribute data to the system—trust that, as noted, cannot be taken for granted given the historical mistrust of government records—. Consistent with the safeguards set forth in the data management section of this document, the profiles must ensure that identifiable data is accessed only when there is a legitimate, explicit, and proportionate purpose, and that such access is logged. Additionally, some of the information may be anonymized to limit certain risks related to privacy, security, or misuse. The aforementioned Inter-American Guidelines of the OAS support this approach by recommending the precise definition of roles throughout the data lifecycle and the adoption of best practices for classifying and categorizing information to ensure its protection[99].

Likewise, this institutional framework must cover not only who manages the system and how data is collected, but also how it is analyzed and what is done with the results, who has access to what type of information and under what accountability and traceability mechanisms, and how data is aggregated or anonymized—which is precisely what distinguishes the system from a simple record of facts. In turn, no decision regarding protective measures or other policies should be made based solely on an algorithm; therefore, these tools must be integrated into a comprehensive strategy that also takes into account context and qualitative variables, and they must be subject to ongoing human oversight.

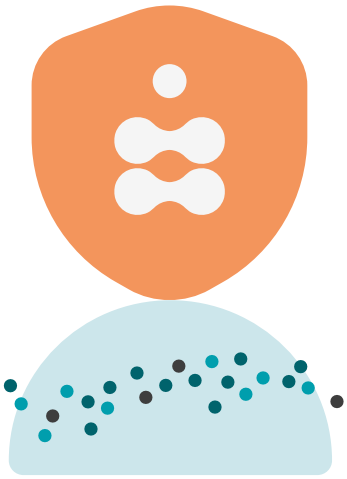
Governance must therefore ensure verifiable mechanisms for auditability, methodological validation, traceability of results, and accountability regarding regulated access to and use of various types of data, so that analytical outputs serve the purpose of protection without reproducing biases, stigmatization, privacy violations, or new forms of persecution, risk, or exposure for the individuals or groups the system seeks to protect[100].

Finally, governance does not allow for a one-size-fits-all design but must be adapted to each country's starting point. Where multiple sources already coexist, the challenge is to coordinate them without forcing their unification or suppressing their autonomy. Where violence against human rights defenders is still not systematically

99 OAS. *Inter-American Guidelines on Data Governance and Artificial Intelligence*, 2024, guidelines 5.4, 6.1, and 6.6

100 OAS. *Inter-American Guidelines on Data Governance and Artificial Intelligence*, 2024, guidelines 5.4, 6.1, and 6.6.

documented, the priority will be to create basic registries that incorporate the necessary safeguards and participation mechanisms from the outset. In both scenarios, the objective is the same—to transform the system into an active infrastructure for prevention and guarantee—but the sequence of governance decisions will vary according to each country's specific context.



XIII. Conclusions

These guidelines aim to address the critical situation faced by many human rights defenders on the continent by fulfilling a clear obligation derived from international and constitutional law: the establishment of a national information system on attacks against human rights defenders.

The process of exploring the implications of the guidelines provided by international law led us to a process of study and learning alongside an interdisciplinary community, aimed at providing essential elements and highlighting the range of possibilities for such systems. The fact is that, in many cases, information already exists. In fact, state and intergovernmental entities, academia, and civil society organizations possess a significant body of relevant data. The shortcoming lies primarily in the way that information is distilled, connected, linked, and used.

Therefore, this document presents a series of minimum recommendations regarding the categories and variables to be considered, the systems available for processing the information, and the results needed to ensure that this information is useful for prevention, individual and collective protection, the investigation of events—using a macro-criminal approach—and accountability.

In an effort not to reinvent the wheel, we conducted in-depth research on existing databases and found a wealth of systematization efforts. However, the absence of relevant information, the limited use of available tools with greater potential, and the lack of adequate interfaces are equally noteworthy. In the *Blueprint*, we sought

to develop the range of available and potential tools, taking into account technical, legal, and public policy considerations based on a keen analysis of the reality and obstacles present on our American continent.

Like many initiatives, this one had a beginning and was supported by a series of key partnerships and contributions from individuals, institutions, and organizations involved in the subject matter. The timeframe was relatively short given the scale of the task. We hope to continue deepening the discussions, collaborative learning, and practical applications of some of the innovations outlined in this document.

This work holds significant potential for addressing a persistent phenomenon that exacts a heavy toll on lives, rights, and the quality of democracies.

We hope this document will serve to guide the implementation of various States' obligations in compliance with constitutional and inter-American rulings and mandates under the American Convention on Human Rights (ACHR) and the Escazú Agreement. Likewise, we hope that these guidelines will facilitate deeper and more interdisciplinary discussions on the subject, thereby refining the tools, practices, and policies of those who bear the fundamental responsibility for respecting and guaranteeing the right to defend rights and for ensuring an enabling environment for its exercise. We also hope that they will help expand and strengthen the essential work carried out by civil society and academia in defending human rights and supporting individuals and communities involved in human rights advocacy.

Once again, we thank those who accompanied this process with generosity, curiosity, and practicality, without ever losing sight of the fact that what is at stake is the real possibility of protecting people, preventing violence, and sustaining more just societies.

Annex I.

Table of Analytical Categories for the Information System

Category and Definition	Subcategory	Variables
1. Defenders / Victims Functional identification of the defender or victim—whether an individual or a group—based on characteristics that help understand the specific risks they face. This is not intended to be an exhaustive census.	**Profile of the human rights defender**	Sex and gender; age; language; ethnic or racial background; sexual orientation; disability; nationality; immigration status; occupation; profession; education; socioeconomic status; place of residence; workplace; organizational affiliation; institutional affiliation; political affiliation; type of leadership; sector or focus of work; history of risk; current or past membership in or association with social movements, organizational processes, or organizations.
2. Events and Types of Attacks Recording of acts and omissions that constitute attacks against human rights defenders and determination of the type of aggression. This includes actions and omissions by the state.	**Type of aggression (action or omission)**	Murder; attempted murder; enforced disappearance; temporary disappearance; arbitrary pretrial detention; criminalization; bodily injury; torture; cruel or inhuman treatment; gender-based violence; sexual violence; sexual torture; slavery; sexual slavery; forced recruitment; confinement; forced displacement; forced eviction; exile; threats; harassment; intimidation; stigmatization campaigns; discrimination; defamation; incitement to violence; doxxing; illegal surveillance; interception of communications; use of spyware or malware; internet shutdowns; deactivation of SIM cards; blocking or disruption of instant messaging; closures or suspensions of organizations; administrative obstacles; indirect restrictions; fines; attacks on headquarters, communities, collective property, and territories.
3. Criminalization Misuse of criminal, civil, or other branches of law by state and non-state actors, with the intent or result of inhibiting, restricting, or silencing the defense of human rights through the manipulation of the state's punitive power.	**Criminalization per se**	Criminalization of conduct protected by freedom of expression (offenses such as contempt, slander, or defamation); punitive actions without legal basis (arbitrary detention, as defined by the Working Group on Arbitrary Detention); use of military jurisdiction to try civilians; prior determination of criminalization by a competent international body (Inter-American Court of Human Rights, Inter-American Commission on Human Rights, Working Group on Arbitrary Detention, or other special procedures or treaty bodies).
	Abuses of the State's punitive power	Abusive use of investigative and prosecutorial powers (multiple investigations or charges, proceedings based on association or membership, vague or aggravated charges); filing of false or unfounded charges; unjustified delay of proceedings (delays, arbitrary sequencing, rescheduling, or late disclosure of charges); imposition of disproportionate precautionary measures (arbitrary pretrial detention, unreasonable surveillance and searches, excessive bail); imposition of disproportionate penalties (excessive fines, dissolution of organizations); violations of due process (restrictions on the right to defense, obstruction of access to legal counsel, withholding of notifications, non bis in idem); abusive use of administrative procedures (entry bans into third countries).

Category and Definition	Subcategory	Variables
→ 3. Criminalization *(continued)*	**SLAPPs (strategic lawsuits against public participation)**	Lawsuits for property damage or trespassing in the context of protests or territorial defense; lawsuits for defamation and other cases related to freedom of expression; litigation arising from protests that affect extractive or infrastructure projects; multiple and simultaneous lawsuits; and the abusive use of amparo (constitutional protection) actions against organizations or human rights defenders.
4. State Response to Risk or Incident State reaction to the risk and the incident: prevention and protection measures and the performance of the justice system.	**Prevention and Protection**	Requests for protection; risk assessments; response time; urgent measures; individual, collective, territorial, or community-based protection schemes; precautionary measures (domestic or issued by the IACHR); provisional measures; review, modification, or termination of protection schemes, with justification; safe return; sufficiency, adequacy, and effectiveness of measures; attacks occurring while measures are in effect; monitoring of institutional early warnings
	Justice and Overcoming Impunity	Procedural timeline (complaints; open or ongoing investigations; indictments; convictions; appeals; final convictions; actual imprisonment; acquittals); levels and networks of responsibility (perpetrators and intellectual perpetrators; chains of command; financiers, accomplices, or actors who acquiesced; levels of planning); guarantees of access to justice and institutional conditions (independence and impartiality; autonomy of investigative and adjudicatory bodies; specialized prosecutors' offices or units; institutional capacity; corruption); consideration of the link to defense efforts; contextual analysis; type of sentence; performance indicators (procedural delays; official statistics on case resolution).
5. Alleged Perpetrators Identification of alleged perpetrators and networks of responsibility, without implying a presumption of guilt; this enables a macro-criminal approach.	**State actors**	Judges; prosecutors; members of law enforcement; public officials; local authorities.
	Non-state actors	Organized armed groups (various illegal groups, paramilitary groups, or other criminal structures, depending on local, national, regional, and global dynamics); individual non-state actors.
	Business actors (legal entities)	Corporations; companies; contractors; third-party funders.
	Forms of coordination	Mixed arrangements; criminal subcontracting; joint action by networks combining state and non-state actors.
6. Context Structural and territorial variables that give meaning to the risk and allow the events to be understood against their broader context.	**Structural variables**	Areas of particular conflict; state absence; presence of legal or illegal armed actors; illicit economies; levels of corruption; regional socioeconomic data; rates of violence (homicide, femicide, injuries, massacres, kidnapping, sexual violence, human trafficking, forced recruitment, slave labor); educational indicators (school enrollment, dropout rates).
	Patterns	Enforced disappearance; persecution; confinement; forced recruitment; deforestation; impunity
	Predictors	Internet shutdowns; sudden and massive population displacements; electoral contexts; environmental permitting processes in countries with weak institutions; disputes among illegal armed groups.

Guidelines for the Development of Information Systems for the Prevention of Crimes Against Human Rights Defenders

Blueprint

Defending rights
to change realities

With more than 30 years of experience, we work to reduce inequality, discrimination, and violence by strengthening democracy, promoting and protecting human rights, and combating impunity in the region. Our mission is to contribute to the full enjoyment of human rights in the Americas through the effective use of the mechanisms of the Inter-American System of Human Rights and other international protection instruments.

We drive these processes alongside victims, organizations, and communities, ensuring they translate into justice, guarantees of non-repetition, and meaningful, lasting change in the region.

www.cejil.org

CEJIL
CENTER FOR JUSTICE AND INTERNATIONAL LAW

ISBN 978-987-23854-9-1