

## ODC's contribution to the Global Digital Compact - Report

# Open Data and the Right to Privacy in a global digital strategy

Author: Renato Berrino Malaccorto

Version date: 30-03-2023

## Content

Introduction/Overview	1
Description of Entity/Organization	2
Methodology/Process	3
Preliminary ideas and definitions	4
Key principles	6
Actions/Recommendations	8
<ul> <li>Democracy strengthening</li> </ul>	8
Technical work	8
Data governance	9
<ul> <li>Data literacy (learning and training)</li> </ul>	9
<ul> <li>Collaboration and engagement (network building)</li> </ul>	9
Regulatory framework	9
Additional ideas	10
Value	10
<ul> <li>Democracy strengthening</li> </ul>	10
Data governance	11
<ul> <li>Collaboration and engagement (network building)</li> </ul>	11
<ul> <li>Innovation</li> </ul>	11
Actors	11
Challenges	12
<ul> <li>Democracy strengthening</li> </ul>	12
• Technical work	12
Data governance	12
<ul> <li>Data literacy (learning and training)</li> </ul>	12
<ul> <li>Collaboration and engagement (network building)</li> </ul>	12
<ul> <li>Regulatory framework</li> </ul>	12



Final remarks	13
Acknowledgments	13
References	14

## Introduction/Overview

Following the political declaration adopted at the occasion of the United Nations' 75th anniversary in September 2020, the Secretary-General in September 2021 released his report Our Common Agenda<sup>1</sup>. The Common Agenda proposes a Global Digital Compact to be agreed at the Summit of the Future in September 2024 through a technology track involving all stakeholders: governments, the United Nations system, the private sector (including tech companies), civil society, grass-roots organizations, academia, and individuals, including youth.

The Global Digital Compact is expected to "outline shared principles for an open, free and secure digital future for all".

The Global Digital Compact proposes the following **thematic axes**:

- Connect all people to the internet, including all schools
- Avoid internet fragmentation
- Protect data
- Apply human rights online
- Introduce accountability criteria for discrimination and misleading content
- Promote regulation of artificial intelligence
- Digital commons as a global public good

Regarding the Global Digital Compact topics, those that will be linked to our contribution are: data protection; application of human rights online; and digital commons as a global public good.

## Description of Entity/Organization

The Open Data Charter (ODC) is a collaboration between over 170 governments and organisations working to open up data based on a shared set of principles<sup>2</sup>. We promote policies and practices that enable governments and CSOs to collect, share, and use well-governed data, to respond effectively and accountably to the following focus areas: anti-corruption, climate action and pay equity.

We want a world in which governments collect, share and use well-governed data, to respond effectively and accountably to our most pressing social, economic, and environmental challenges. We want this to happen by default unless it would demonstrably infringe human rights.

Specifically, we want:

1

https://www.un.org/en/content/common-agenda-report/assets/pdf/Common\_Agenda\_Report\_English.pdf

<sup>&</sup>lt;sup>2</sup> <u>https://opendatacharter.net/principles/</u>



- public officials to balance the tradeoffs between advancing transparency and accountability using data and protecting the rights of people and communities
- citizens to be able to easily see and influence what their public officials do, and to trust their institutions
- people to be able to use openly available data and accountable automated tools to access equitable public services

The ODC is setting up a participatory process to send inputs to the Global Digital Compact. The Organization is working on the data rights and digital rights agenda, with a strong focus on access to public information, open data and dialogue with the right to privacy. It is doing research in good practices and regulatory advances, and generating resources to support the community.

The ODC promotes research to understand the balance of these rights in specific thematic axes, and see how they dialogue in specific cases. In addition, we analyze good practices and lessons from different forms of data protection regulation, with a specific focus on how this affects open data, to generate public policy recommendations.

## Methodology/Process

The ODC is contributing to the Global Digital Compact conducting an analysis and debate to help understand access to information and open data as a fundamental human right, in balance with the right to privacy.

In order to share our input, we are using a mixed methodological approach.

First of all, we have done desk research about national and international regulations on access to public information, open data and the right to privacy. In addition, we consulted principles and reports produced from different organizations and stakeholders.

As a second step, we have invited key stakeholders on the subject of Open Data and the Right to Privacy to inform the contribution report. We conducted two consultation sessions via Zoom. 17 organizations (see *acknowledgments*) that work on Open Data, Access to Information, Digital Rights and on Right to Privacy joined the discussion and shared their ideas. The session was structured in the following sections: Opening remarks: context and objective; Initial ideas on open data and privacy; Collective discussion.

For the collective discussion, we worked together in a jamboard trying to answer the following proposed questions:

- 1. Why should access to information and open data be included in a global digital strategy? -This question led us to discuss the VALUE of the institutes.
- 2. What shared tools or principles do you know to balance openness and the right to privacy? -This question led us to explore PRINCIPLES.
- What are the challenges to achieve this balance between openness and respect for privacy?
   This question led us to understand the CHALLENGES.
- 4. Which actors should not be missing in the conversation regarding the balance of Open Data and the Right to Privacy? This question helped us to identify key ACTORS.



5. What specific actions and/or policies would we need to guarantee this balance without compromising any of the rights? What can and should the international community do about it? - This question helped us to come across ACTIONS.

Although in the research and consultation we have worked more broadly to contextualize and better understand the balance between the institutes, the contribution to the Pact is mainly divided into: 1) Principles; 2) Actions

- Principles: core principles that all governments at the national and sub- national level, companies, civil society organizations, and other stakeholders should adhere to.
- Actions: key commitments to bring about these specific principles. These can take the form of what participants think "should" be done, and/or based on what their organization has already committed to do.

The resulting document, prior to submission, is also open for public consultation in an online platform<sup>3</sup> during March 2023. In addition, the document was shared with all the participants that joined the session for additional comments or views.

Finally, the contribution to the Global Digital Compact will be sent before March 31, 2023.

The UN will present the contributions at the Summit of the Future in 2024.

## **Preliminary ideas and definitions**

Access to public information is internationally understood as a fundamental human right (for example, the United Nations Human Rights Committee recognizes it in its general comments on article 19 of the Universal Declaration of Human Rights when analyzing freedom of expression<sup>4</sup>). The fundament is that it allows citizens and interested parties to be informed and exercise other rights, functioning as a key right.

There are regulations in different countries and regions that have contemplated and regulated it for many years. In many cases, it is even included in the Constitutions, as is the case of Spain or Portugal. In Sweden, for example, the right was recognized for centuries, but most European countries have regulated it in the last 50 years<sup>5</sup>, while in Latin America it has been legislated around 30 years ago, but has had a deeper development in the last decade.

According to the Organization of American States (OAS), the Economic Commission for Latin America and the Caribbean (ECLAC), and various compared regulations, the **Right of Access to Public Information** is understood as: "the ability to search, access, freely request, receive, copy, analyze, reprocess, reuse and redistribute the information under the custody of the Public Authority."

In recent years, with the development of Information and Communication Technologies (ICTs) and digitalization, the way in which information is produced, published and shared has changed, becoming mostly digital data. The changes range from the way in which data is produced, published and safeguarded, to how citizens access and interact with it. In this context, we find the importance of

<sup>&</sup>lt;sup>3</sup> The public consultation will be held in

https://odc.pubpub.org/pub/ggt0ptuu/draft?access=m2j2lpoc

<sup>&</sup>lt;sup>4</sup> <u>https://www2.ohchr.org/english/bodies/hrc/docs/GC34.pdf</u>

<sup>&</sup>lt;sup>5</sup> <u>https://research.mysociety.org/publications/improving-oversight</u>



**Open Data**<sup>6</sup> as a superior instance in the digital era, understanding it as *digital data that is made available with the necessary technical and legal characteristics so that it can be used, reused and redistributed freely by anyone, anytime, anywhere.* It is important to mention at this instance that where there are no regulations on open data yet, the Right of Access to Information framework is what shapes these policies.

The Right of Access to Public Information is, today, intrinsically linked to the concept of Open Data. Various compared regulations and the Inter-American Model Law 2.0 on Access to Public Information<sup>7</sup> establish that access to information must be in open data format, incorporating it as the appropriate way to exercise the right, within the framework of **proactive transparency**.

These regulations contain provisions that regulate the duty of States to publish certain categories of information without a request for information (what is known as **passive transparency**). Article 5 of the Inter-American Model Law on Access to Information establishes the obligation to "proactively disseminate the key Information established in this Law, without a request for this Information". In its second paragraph, it also establishes that "every obligated subject must allow the widest access to Information, in such a way that it allows its interoperability in an open data format, as well as determine the strategies for the identification, generation, publication organization and dissemination of that Information that must be proactively published (information on the obligated subject, information on officials, financial information, citizen participation mechanisms, and needs of specific groups). In addition, it establishes obligations, publication schemes, and the obligation to guarantee and provide applicants with access, in the easiest way possible, to all previously disclosed documents. Proactive transparency obligations are found in many legal systems around the world, and the incorporation of the concept of open data often occurs in the Law on Access to Information itself, or in complementary regulations.

The proactive publication of information in open data format allows improvements in various aspects. On one hand, it avoids the expense of resources in answering requests for access to information, when it is information that must be open by default, and it saves time for the citizen as they don't need to make the request. Working on open data implies, in addition to openness, improvements in internal processes, since work is being done on the production and normalization of data with standards, update periods, etc. Likewise, from the organization, and within the framework of the Charter, we talk about the need for data to be open with a purpose: openness strengthens citizen participation, public policies, public management and therefore democratic governance. Open data contributes to innovation and to tackling the biggest public challenges of this century. Openness empowers citizens to participate both in decision-making and in the monitoring of public policies.

Data is a key part of the fabric of today's societies and economies. How we access, use and regulate data is more important than ever. Used effectively, open data makes governments more efficient and transparent and empowers citizens to participate and be part of public accountability. However, this production and availability of data and information brings to the table the need to discuss the responsible management of the data and the protection of personal and/or sensitive data.

<sup>&</sup>lt;sup>6</sup> <u>https://opendatacharter.net/principles/</u>

https://www.oas.org/es/sla/ddi/docs/publicacion\_Ley\_Modelo\_Interamericana\_2\_0\_sobre\_Acceso \_Informacion\_Publica.pdf



It is important to understand that when we talk about transparency and open data, as well as the protection of personal data and privacy, we are talking about issues directly linked to human rights. In this case, when talking about data, we can circumscribe it to the universe of human rights applied to the digital sphere, commonly known as digital rights, which is part of our current daily life.

The **right to privacy** is contemplated in various international instruments<sup>8</sup> and in the Constitutions of numerous countries around the world. It is a fundamental human right, and in the digital age, it takes on new dimensions. It is in this context of massive data production and circulation that great advances have been necessary in terms of personal **data protection regulation** in recent years. The personal data protection prevents and defends people from arbitrary or illegal interference in their private life, family, home or correspondence. Various countries have had legislation on this topic for years, and many regulations are in the process of being updated to be adapted to the realities of new digital environments. Since 2018, the topic has become specially relevant due to the General Data Protection Regulation (GDPR) of the EU<sup>9</sup>. A particularity of this regulation is that it incorporates the right that grants subjects the possibility of accessing all the data stored about them within public and private sector entities, similar to the "Habeas Data" guarantee action, incorporated in various legal systems.

The GDPR defines **personal data** as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. **Data protection** refers to the practices, safeguards, and binding rules put in place to protect your personal information and ensure that you remain in control of it. The regulation identifies diverse **personal data rights**: information, access, rectification, restrict processing, erasure, object, explanation, data portability.

The importance of the right to access to information and the right to personal data protection, both of which are fundamental human rights, raises the need to strike a balance to be able to exercise both in a complementary manner, that ensures that one of them does not jeopardize the guarantees enshrined by the other. There are different proposals and techniques that allow us to continue working on open data for a more democratic and just society, respecting the right to privacy. We explored some ideas on the consultation sessions, expressed below.

## Key principles

During the consultation sessions, we identified different principles, by collectively answering the question: what shared tools or principles do you know to balance openness and the right to privacy?

We understand principles as core practices that all governments, companies, civil society organizations, and other stakeholders should adhere to.

Below we share the principles we worked on:

<sup>&</sup>lt;sup>8</sup> <u>https://www.ohchr.org/en/special-procedures/sr-privacy/international-standards</u>

<sup>&</sup>lt;sup>9</sup> <u>https://adpr-info.eu/</u>



- In terms of open data, **ODC proposes 6 principles**<sup>10</sup>. To these principles we should add the idea of opening data with purpose.
- Inclusive human rights impact assessments and participatory technology assessments.
- **Trust:** that data is accurate and stored securely. The data collection must be proportional and necessary. This ensures that human rights are respected and that data collection is done ethically and legally. That's the necessary first stop for it to be reused and shared. There's a need to count on trust mediators, and national commissions for regulation or trust-building.
- Necessary **dialogue between Open by default and Privacy by design**. Both of them can coexist if we make opening plans in advance.
- Digitally/culturally appropriate **consent**, **grievance and complaint mechanisms**.
- **Risk assessment** tools that also engage with risks at collective levels. This is where non-PII (Personal Identifying Information) open data have to be assessed. Understanding, acknowledging and identifying collective risk/group risk/intersectional risk is necessary.
- **Participatory deliberative processes** to establish contextually appropriate regulation (including the use of existing toolkits for non-expert engagement).
- **Data Sovereignty** that goes beyond an individual's rights towards their data (PII) to also include groups' collective rights towards data that is about them or affects them. Only with collective digital sovereignty enabled can we have collective decision-making about publishing with a purpose.
- Other principles shared by the participants: Security by Design (SbD)<sup>11</sup>. Data Minimization Principle<sup>12</sup>, Principle of maximum publicity.
- In addition, the participants shared different principles that already exist and have been developed by different organizations, for example: FAIR principles<sup>13</sup>; CARE principles<sup>14</sup>; ICO Guidance<sup>15</sup>; The Five Safes<sup>16</sup>; The ODI Data Spectrum<sup>17</sup>; The public interest test<sup>18</sup>; Trusted Research Environments<sup>19</sup>; MyData principles<sup>20</sup>; Foundation for Public Code [guide]<sup>21</sup>; Human Rights Council "resolution on the promotion and protection of human rights on the internet"<sup>22</sup>; The Global Principles on Protection of Freedom of Expression and Privacy<sup>23</sup> from Article 19;

<sup>&</sup>lt;sup>10</sup> <u>https://opendatacharter.net/principles/</u>

https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specificationscamss/solution/elap/security-design

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection \_regulation-gdpr/principles/data-minimisation/

<sup>&</sup>lt;sup>13</sup> <u>https://www.go-fair.org/fair-principles/</u>

<sup>&</sup>lt;sup>14</sup> <u>https://www.gida-global.org/care</u>

<sup>15</sup> 

https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-call-for-views-anonymisation-n-pseudonymisation-and-privacy-enhancing-technologies-guidance/

<sup>&</sup>lt;sup>16</sup> https://blog.ons.gov.uk/2017/01/27/the-five-safes-data-privacy-at-ons/

<sup>&</sup>lt;sup>17</sup> <u>https://www.theodi.org/about-the-odi/the-data-spectrum/</u>

<sup>18</sup> 

https://ico.org.uk/for-organisations/guidance-index/freedom-of-information-and-environmental-information-regulations/the-public-interest-test/

<sup>&</sup>lt;sup>19</sup> https://www.hdruk.ac.uk/access-to-health-data/trusted-research-environments/

<sup>&</sup>lt;sup>20</sup> <u>https://www.mydata.org/participate/declaration/</u>

<sup>&</sup>lt;sup>21</sup> https://publiccode.net/ and https://github.com/openstate

<sup>&</sup>lt;sup>22</sup> <u>https://www.ohchr.org/en/stories/2013/10/right-privacy-digital-age</u>

<sup>&</sup>lt;sup>23</sup> https://www.article19.org/data/files/medialibrary/38657/Expression-and-Privacy-Principles-1.pdf



Data Ethics Canvas of the Open Data Institute (ODI)<sup>24</sup>; the principles of Data Ethics in the Public Sector of the OECD<sup>25</sup>; and the UK data ethics framework<sup>26</sup>, Necessary and Proportionate of the EFF <sup>27</sup>. The ODI Canvas, for example, is a valuable tool that guides us in data collection, use and publication processes, proposing a series of items to think about in the development of projects: identify data sources, their limitations, the possibilities of sharing this data or not, the ethical and legislative context, identifying the rights linked to these data sources, the positive and negative effects that it can have on citizens, communication, among other points.

It is important to highlight that some participants share the idea that principles alone are not enough<sup>28</sup>. This is why a comprehensive strategy is necessary, with concrete actions and policies, and taking into consideration challenges and actors.

## Actions/Recommendations

During the consultation sessions, we identified actions and recommendations, by collectively answering the questions: What specific actions and/or policies would we need to guarantee this balance without compromising any of the rights? What can and should the international community do about it?

We understand actions as key commitments to bring about these specific principles. These can take the form of what participants think "should" be done, and/or based on what an organization has already committed to do.

Below we share the actions we reflected on:

#### • Democracy strengthening

- Development and respect of digital sovereignty principles
- Exploring trusted research environments and data trusts/intermediaries.
- It is not enough to focus on data protection, we need to look beyond the protection of Privacy and its inclusion in the design of all policies and programs. For this, Human Rights Impact Assessments (HRIA) are an excellent tool that can guide policy- making at every level of government.
- A statement or report from the Rapporteurs on this topic would be a necessary tool.
- Context matters. The balance between these rights varies and dialogues in different ways according to the types of data we are working with and sectorial topics that are addressed.
- Technical work
  - Work on data standards and data assurance. This is specifically important to ensure interoperability. The more quality datasets you have access to, and the easier it is for

<sup>&</sup>lt;sup>24</sup> <u>https://theodi.org/wp-content/uploads/2019/07/ODI-Data-Ethics-Canvas-2019-05.pdf</u> <sup>25</sup>

https://www.oecd.org/digital/digital-government/good-practice-principles-for-data-ethics-in-the-public-sector.htm

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\_data/fil e/923108/Data\_Ethics\_Framework\_2020.pdf

<sup>&</sup>lt;sup>27</sup> https://necessaryandproportionate.org/es/13-principles/

<sup>&</sup>lt;sup>28</sup> <u>https://www.nature.com/articles/s42256-019-0114-4</u>



them to talk to each other, the more potential value you can get from them. Commonly-agreed data standards play a crucial role in making this happen.

- Define clear objectives in transparency and open data policies. It is key to make opening plans, taking into account current regulations, demand, resources, etc. In this way, when planning, risks can be identified and if there is personal or reserved information, it can be treated to avoid publishing data that does not correspond, and to be able to publish the rest of the information with the necessary precautions. Planning ahead is important to identify risks, prevent and mitigate them.
- Apply data protection techniques. Regarding personal data, there are anonymization guides to be able to open data protecting private and/or sensitive information.
- Intersectional analysis regarding needs, priorities, risks of groups and populations in a situation of greater vulnerability.

#### • Data governance

- Work on better data governance regulations. Regulators should be better informed about data and data-enabled systems.
- Clarify decisional structures, roles, and responsibilities, how the decisions are taken and communicate.
- Expansive data governance<sup>29</sup> frameworks that include all stakeholders.
- Need of control authorities/oversight bodies with hierarchical equality. These actors must be independent from the State. Regarding public governance structures, it is important that the Oversight Bodies for the application of the laws on access to public information and protection of personal data, whether they are under the same orbit or not, work in synergies in the safeguarding of both rights to guarantee them.
- Coordination within the UN itself on who is handling the topics (multiple agencies handling similar issues does not help coordination).

#### • Data literacy (learning and training)

• Establish relational mechanisms to facilitate collaboration between individuals and organizations involved through communication, training, and coordination. There's a need for data literacy initiatives. Create a shared understanding and a shared vocabulary, have a clear answer with examples on the benefits such a balance can bring.

#### • Collaboration and engagement (network building)

- Community engagement and participatory data governance structures and processes. Guidelines for national implementation of empowering and people-focused data regulatory frameworks. There's a need to involve the public. We should develop and implement citizen awareness strategies. A good idea would be to coordinate events that bring together the communities of practice and authorities that carry out these agendas, in general there are conversations in silos.
- Work on pilots that can demonstrate the value of data use.

#### • Regulatory framework

- User rights clarity and policies that follow these. There's a need for information on rights in more user-friendly formats.
- Regulatory harmonization and balance. It is important to understand the current regulations and how they dialogue with each other, both locally, nationally, and internationally, in order to make effective and balanced rights without detriment to any of them. The legal system must be coherent and harmonious. Participants

<sup>&</sup>lt;sup>29</sup> <u>https://training.lms.opennorth.ca/catalog/info/id:176</u>



identified a need for data protection law in countries that do not have them: the Global Digital Compact can recommend the adoption of these laws. Data Protection laws and Access to Information laws (or Open Data policies) must dialogue with each other. They specify what information is personal and confidential, and provide alternatives for its publication with different techniques. A good example is the Model Law on Access to Information 2.0 of the Organization of American States<sup>30</sup>, which contemplates confidential information and personal data, and how information can be processed or shared partially with consent. The GDPR, in the same way, points that public access to official documents must be reconciled with the right to the protection of personal data.

Another reflection brings to the table that we cannot "guarantee" the balance and shouldn't aim to, that's setting ourselves up for failure. This is a dynamic environment and should be treated as such. It is important to be aware of the context and adapt the strategies to it. It doesn't mean that we are going to leave the window open to failures that harms rights, but we have to be aware that the context changes every time, and that our process and strategies should be considered "unfinished", so that we can rethink and adapt them to work better and more effectively in the human rights defense.

In addition, other participants suggest that it is important to think that in parallel to these topics, we have to continue raising the issue of connectivity and digital inclusion.

## Additional ideas

Although the contribution to the Pact is mainly divided into principles and actions, in the research and consultation we have worked more broadly to contextualize and better understand the balance between the institutes. More ideas on the topics are shared in this section.

#### Value

During the consultation sessions, we reflected on the value of the institutes. by collectively answering the question: Why should access to information and open data be included in a global digital strategy?

Below we share the ideas we worked on:

#### • Democracy strengthening

- Enables the design, evaluation and monitoring of policies, It ensures accountability. Access to public information is a fundamental pillar of a democratic system.
- These rights are part of the digital ecosystem and are part of the different democracies, therefore it requires global protection when developing on the internet.
- They are key institutional axes to enable the right to know.
- They nurture trust between the state and citizens.
- It helps to fight disinformation.
- Data availability and accountability are critical to the success of a digital strategy. Any "global digital strategy" should be related to the "datafication" process of society,

<sup>30</sup> 

https://www.oas.org/es/sla/ddi/docs/publicacion\_Ley\_Modelo\_Interamericana\_2\_0\_sobre\_Acceso \_Informacion\_Publica.pdf



which includes public open data. Public data feeds this process and the public-private flow, which supports/drives/promotes/exploits the datafication process.

- These rights help to level the playing field allowing less powerful actors to also access quality data. Different groups in society should have an equal information position and actively work on improving the quality of this information for the benefit of society. A particular attention to marginalized and vulnerable communities such as women, lgtbqi plus groups, rural communities and other groups should be prioritized in a level playing field strategy promoted by the State.
- Important to inform the decision-making processes.
- They allow strengthening civil society in discussions of public affairs.
- It is important to understand the digital commons as a public good.
- The Right to access information has a digital way of implementing it so to have it as a part of a Global Digital Strategy it is also a way to help guarantee that Right.

#### • Data governance

• It is important because this and other Internet governance processes (global and national) must be transparent and participatory. Open data is fundamental to structure public data governance.

#### • Collaboration and engagement (network building)

- To accelerate knowledge transfer. It encourages collaboration across multi sectoral organizations and facilitates new findings.
- Understanding what data/information people want can help inform design.

#### • Innovation

- Open data allows data and information made with public money to revert to society to be able to use it as best as is convenient.
- Improves the delivery of goods and services.

#### Actors

During the consultation sessions, we worked identifying key actors. by collectively answering the question: Which actors should not be missing in the conversation regarding the balance of Open Data and the Right to Privacy?

Below we share actors we agreed on:

- Civil society/community groups. It would be important to count with the participation of organizations that are focused on particular sectors (e.g. health, education), not just data.
- Research community and academic experts across the social sciences and humanities.
- Public sector officials collecting and sharing data. In particular: Data protection officers and Information commissioners; Statistical offices; Oversight bodies.
- Private sector, specially big techs and startups.
- Data journalists.
- Judges specialized in habeas data and similar processes.
- UN agencies handling the agenda<sup>31</sup> (eg. UNESCO, OCHCR, UN stats, ITU and more sectorial conversations with UNICEF, UN-Habitat, UN Women, WHO, WFP, UNDP).

<sup>&</sup>lt;sup>31</sup> There's a mapping of UN strategies/policies in digital rights in the first chapter of this guide: <u>https://unhabitat.org/mainstreaming-human-rights-in-the-digital-transformation-of-cities-a-guide-fo</u> <u>r-local-governements</u>



In addition, the participants reflect that it's not enough to just passively open up the conversation. Marginalized communities deserve proactive engagement.

Another interesting reflection mentions that the discussion It's also about how to build the understanding and the opportunities so people can join the conversation.

#### Challenges

During the consultation sessions, we worked to understand the challenges. by collectively answering the question: What are the challenges to achieve this balance between openness and respect for privacy?

Below we share the challenges we identified:

#### • Democracy strengthening

- The two poles that generate tension have legitimate interests (protecting privacy / generating more useful information). A first challenge is to be aware of that.
- Citizens' trust in governments may deteriorate if their information is not used appropriately.
- Technical work
  - Working with stakeholders' differential intersectional risk assessments, i.e. not assuming that all stakeholders will have the same risk profiles. PII legislation tends to fail to grasp this differentiality, e.g. anonymous mobility data is still a risk to persecuted minorities.
  - Some accountability/transparency data (public sector salaries, beneficial ownership registers) involve data about individuals. There's a need to explore how we can work and access this data without compromising personal data protection. There are different techniques that can help us.
  - The lack of analysis of the impact on rights when innovation projects or the incorporation of technology in the public service are implemented.
  - Depending on the context and the granularity of the data, there are situations in which its anonymization becomes impossible. There's a need to find solutions for these cases.

#### • Data governance

- Finding the right data stewardship model that can help balance.
- There may be a Data Protection Officer and an Information Commissioner at one digital policy-making department in governments; we need to create a tool to make them collaborate/discuss. Oversight bodies must work in synergies. And must be independent.

#### • Data literacy (learning and training)

- Data literacy of people whose data are being used. Communities in silos not sensitized to either openness or privacy (open optimists vs. privacy fatalists).
- Jigsaw identification<sup>32</sup>.
- Collaboration and engagement (network building)
  - Individualistic conceptions of data can ignore a) other people's privacy and b) collective harms/benefits.

<sup>&</sup>lt;sup>32</sup> <u>https://www.igi-global.com/dictionary/jigsaw-identification/74722</u>



#### • Regulatory framework

- Lack of regulatory alignment and public policies for openness and data protection (and other related topics such as cybersecurity and artificial intelligence).
- Misinterpretation and application of standards and regulations on the protection of personal data or massive copy paste of regulations from other contexts. Context matters.
- Privacy is too easily used as an excuse not to be open. There's a misinterpretation of norms.
- The absence of regulation on the use of public data (not open) as sources for OSINT<sup>33</sup> and the limits of this type of research for States.
- Government agencies that have data do not feel the need to share it if there is no regulatory framework to mandate it.

Another interesting contribution highlights that there is no silver bullet or one-size-fits-all model, communities must be able to define this balance for themselves.

Another participant suggests that it is interesting to consider that the main challenge is about power. The powerful needs greater openness (so we have accountability) and the weakest need more privacy (to avoid exploitation)

There's another challenge identified that has to do with apathy and lack of interest from citizenship, often generated by mistrust.

## Final remarks

In this report, after doing research and a consultation process with key actors, we proposed core principles and key commitments that should be taken into consideration to incorporate Open Data and the Right to Privacy in a Global Digital Strategy.

In addition, we explored ideas on the value of Access to Information and Open Data. the actors that should not be missing in the conversation regarding the balance of Open Data and the Right to Privacy, and the challenges we are facing.

For the reasons explained above, we believe that Open Data and the Right to Privacy are not only complimentary, but must be understood in harmony when practiced, in order to protect fundamental human rights. There are different regulations, guides and principles that help us to balance this situation and push us to achieve coherence in the development of public policies.

We hope this contribution will nurture the Global Digital Compact, with the objective to achieve an open, free and secure digital future for all. As a follow-up to this project we will definitely be keeping this conversation alive so that we can deepen the exploration of data rights to find the right balance.

## Acknowledgments

The following collaborators joined us for the discussion sessions. We thank them for their participation, insight, and review of this report.

<sup>&</sup>lt;sup>33</sup> <u>https://osintframework.com/</u>



- Open Data Institute: Gavin Freeguard
- MyData Global: Christopher Wilson and Viivi Lähteenoja
- Open North: Thomas Linder and Marie Plamondon
- International Development Research Centre: Fernando Perini
- Global Data Barometer: Silvana Fumega
- Cities Coalition for Digital Rights: Florencia Serale and Milou Jensen
- The Engine Room: Lesedi Bewlay
- IADB: Evelyn Molina Bolanos
- Social TIC: Juan Casanueva
- Hiperderecho: Dilmar Villena
- Fundación Internet Bolivia: Wilfredo Jordan
- Association for Progressive Communication: Paula Martins
- TEDIC: Eduardo Carrillo and Maricarmen Sequera
- Fundación Karisma: Pilar Saenz and Juan de Brigard
- Centro de Estudios en Libertad de Expresión y Acceso a la Información: Ramiro Álvarez Ugarte and Lina Vazquez
- Article 19: Martha Tudon
- Open Data Charter: Mercedes de Los Santos and Natalia Carfi.

### References

Article 19 (2017). The Global Principles on Protection of Freedom of Expression and Privacy. Retrieved from:

https://www.article19.org/data/files/medialibrary/38657/Expression-and-Privacy-Principles-1.pdf

Electronic Frontier Foundation (2013). Necessary and Proportionate. Principles on the application of human rights to communications surveillance. Retrieved from: https://necessaryandproportionate.org/es/13-principles/

Global Indigenous Data Alliance (2022). CARE principles for indigenous data governance. Retrieved from: <a href="https://www.gida-global.org/care">https://www.gida-global.org/care</a>

Go FAIR (2016). FAIR Guiding Principles for scientific data management and stewardship. Retrieved from: <u>https://www.go-fair.org/fair-principles/</u>

Government Digital Services UK (2020). Data Ethics Framework. Retrieved from: <u>https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\_data/file/923108/Data\_Ethics\_Framework\_2020.pdf</u>

Health Data Research UK. Trusted research environments. Retrieved from: <u>https://www.hdruk.ac.uk/access-to-health-data/trusted-research-environments/</u>

Information Commissioner's Office UK. The public interest test. Retrieved from: https://ico.org.uk/for-organisations/guidance-index/freedom-of-information-and-environmental-inf ormation-regulations/the-public-interest-test/

MyData (2017). Declaration of MyData Principles. Retrieved from: <u>https://www.mydata.org/participate/declaration/</u>



My Society (2022). Improving oversight of Access to Information. Learning from different approaches<br/>acrossEurope.Retrievedfrom:https://research.mysociety.org/html/improving-oversight/improving-oversight.pdf

OECD. Good Practice Principles for Data Ethics in the Public Sector. Retrieved from: <u>https://www.oecd.org/digital/digital-government/good-practice-principles-for-data-ethics-in-the-public-sector.htm</u>

Office for National Statistics UK (2017). The 'Five Safes' – Data Privacy at ONS. Retrieved from: <u>https://blog.ons.gov.uk/2017/01/27/the-five-safes-data-privacy-at-ons/</u>

OHCHR (2013). The right to privacy in the digital age. Retrieved from: <u>https://www.ohchr.org/en/stories/2013/10/right-privacy-digital-age</u>

Open Data Charter (2015). International Open Data Charter. Retrieved from: https://opendatacharter.net/wp-content/uploads/2015/10/opendatacharter-charter\_F.pdf

Open Data Institute. The Data Spectrum. Retrieved from: <u>https://www.theodi.org/about-the-odi/the-data-spectrum/</u>

Open Data Institute (2019). Data Ethics Canvas. Retrieved from: <u>https://theodi.org/wp-content/uploads/2019/07/ODI-Data-Ethics-Canvas-2019-05.pdf</u>

Organization of American States (OAS) (2020). Inter-American Model Law 2.0 on Access to Information. Retrieved

https://www.oas.org/es/sla/ddi/docs/publicacion\_Ley\_Modelo\_Interamericana\_2\_0\_sobre\_Acceso \_Informacion\_Publica.pdf

UN Habitat (2022). Mainstreaming human rights in the digital transformation of cities – A guide for local governments. Retrieved from: https://unhabitat.org/mainstreaming-human-rights-in-the-digital-transformation-of-cities-a-guide-fo r-local-governements

United Nations Human Rights Committee (2011). General comments on article 19 of the UniversalDeclarationofHumanRights.Retrievedfrom:https://www2.ohchr.org/english/bodies/hrc/docs/GC34.pdf

United Nations. Report of the Secretary-General (2021). Our common agenda. Retrieved from: <a href="https://www.un.org/en/content/common-agenda-report/assets/pdf/Common\_Agenda\_Report\_English.pdf">https://www.un.org/en/content/common-agenda-report/assets/pdf/Common\_Agenda\_Report\_English.pdf</a>