Law . Legislation . Open Government . Access to Information . Open Data

Legal Aspects of Open Government and Open Data

UNITED NATIONS
الاسكوا
ESCWA

Shared Prosperity **Dignified Life**

UNITED NATIONS
الاسكوا
ESCWA

Shared Prosperity **Dignified Life**

VISION

ESCWA, an innovative catalyst for a stable, just and flourishing Arab region

MISSION

Committed to the 2030 Agenda, ESCWA's passionate team produces innovative knowledge, fosters regional consensus and delivers transformational policy advice. Together, we work for a sustainable future for all.

Distr.
LIMITED
E/ESCWA/CL4.SIT/2020/TP.2
27 March 2020
ENGLISH
ORIGINAL: ARABIC

Economic and Social Commission for Western Asia (ESCWA)

Legal Aspects of Open Government and Open Data

United Nations
Beirut

United Nations publication issued by ESCWA, United Nations House, Riad El Solh Square, P.O. Box: 11-8575, Beirut, Lebanon.

Website: www.unescwa.org.

Photo credit: ©iStock.com

Acknowledgements

The present report was prepared within the framework of a project entitled “Fostering Institutional Development for Participatory Approaches towards the Achievement of the Sustainable Development Goals in Western Asia”. The Innovation Section of the Technology for Development Division of the Economic and Social Commission for Western Asia (ESCWA) participated in this project, with a focus on promoting open government in Arab countries, through the use of and adaptation to modern and emerging technologies.

The report was prepared by Mr. Khaled Sallami, Director General of the -e-Government Unit of the Tunisian Prime Ministry. Ms. Nibal Idlebi, Chief of the Innovation Section of the Technology for Development Division, oversaw its preparation and peer review. Mr. Mohammad Nahar, ESCEA Innovation Department, made valuable contributions to the review process.

Contents

List of tables

List of figures

List of boxes

I. Open Government and Open Data

A. Open government

The concept of open government has emerged in recent years as a new form of governance that Governments are racing to implement. This concept is based on the principles of good governance, such as transparency of government action; realizing the right of citizens to access government information; involving citizens in policy development and decision-making; and establishing mechanisms to hold Governments accountable.

The concept of open government is distinguished by its many dimensions. There is no single definition of open government, as the meaning of this term and its related concepts are in constant flux as a result of new ideas, visions and goals. Many global institutions concerned with transparency and openness, such as the World Wide Web Foundation, have coined a standard definition of the concept of open government. Moreover, many international organizations have addressed the topic of open government, including the World Bank, the Organization for Economic Cooperation and Development (OECD), the United Nations Department of Economic and Social Affairs and ESCWA, and have contributed to defining concepts of open government and implementing activities related to them.

The World Wide Web Foundation defines open government as rethinking how to govern, and rethinking how the administrations should adapt their procedures to meet the demands and necessities of the citizens. Open Government means a cultural, organizational, procedural and attitude change in public servants and the relation with the citizens. It is a new form of understanding political policies which are more legitimate and collaborative. Open Government = Transparency + Efficiency + Participation + Accountability.[1]

The United Nations Development Programme believes that strengthening core government functions, through more openness to better manage and deliver public resources, is a key strategy to keep people out of poverty. Moreover, open government helps bolster the integrity and inclusiveness of government institutions - two essential prerequisites for leaving no one behind.[2]

Open government is one of the main pillars that support the implementation of the Sustainable Development Goals (SDGs), especially Goal 16 on promoting peaceful and inclusive societies for sustainable development, providing access to justice for all and building effective, accountable and inclusive institutions at all levels.[3]

---

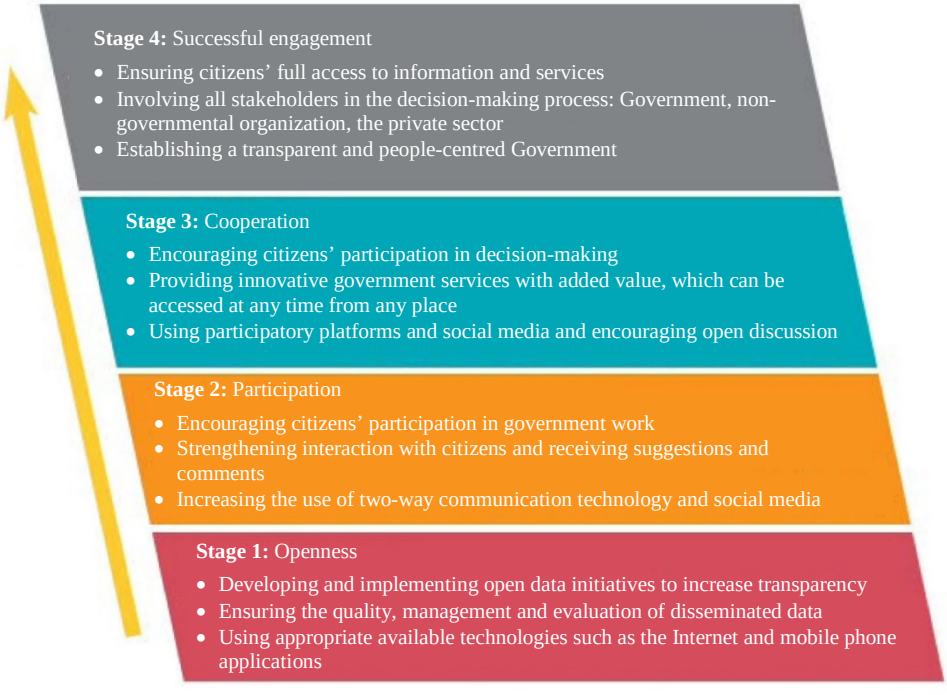
[1] World Wide Web Foundation, Open Government Data Feasibility Studies. Available at https://webfoundation.org/our-work/projects/open-government-data-feasibility-studies (accessed on 30 March 2020).

[2] United Nations Development Programme, Open government is the key to leaving no one behind, https://www.undp.org/content/undp/en/home/blog/2018/open-government-is-the-key-to-leaving-no-one-behind.html (posted on 16 July 2018).

[3] UNDP Arab States, Goal 16: Peace, justice and strong institutions. Available at https://www.arabstates.undp.org/content/rbas/en/home/sustainable-development-goals/goal-16-peace-justice-and-strong-institutions.html (accessed on 30 March 2020).

ESCWA defines open government as a Government that is effective and efficient in carrying out its duties, its work is transparent and accountable, and everyone can access its services. It is also a Government that responds to the needs of its citizens, values their participation, experience and knowledge in decision-making, and relies on modern and emerging technologies to enhance its governance. ESCWA believes that improving participation, transparency and accountability are the primary goals of open government, regardless of its definition.[4] ESCWA has proposed a framework for implementing open government, in line with Arab countries' specificities, comprising the following stages: openness, participation, cooperation and successful engagement.

Figure 1. ESCWA proposed framework for implementing open government



Source: ESCWA, Fostering open government in the Arab region, 2018. E/ESCWA/TDD/2018/INF.1.

1. *Open Government Partnership*

The Open Government Partnership is the first initiative to institutionalize and organize cooperation in the field of open government. It is a multilateral initiative announced by eight countries at the annual opening session of the United Nations General Assembly in New York in 2011. A total of 80 countries participate in this initiative today, alongside numerous non-governmental organizations and several major cities that have been accepted in this partnership to expand its scope at the regional level. The initiative aims to perpetuate the principles of open government worldwide. According to the Open Government Partnership, these principles are:

[4] E/ESCWA/TDD/2018/INF.1.

- Supporting transparency: by cementing the right to access information, and by opening government data and making them available;

- Encouraging citizen participation: in the public decision-making process and in formulating government policies and programmes to ensure that they meet citizens' needs;

- Strengthening accountability: by fighting corruption and promoting integrity;

- Using information and communications technology to disseminate these principles.

2. *Criteria for joining the Open Government Partnership*

Joining the Open Government Partnership requires meeting a number of criteria, including adopting several laws and regulations, as follows:

- Financial and fiscal transparency: publishing budget reports and approving an open budget;

- Right to access information: adopt a law to access information and include this right in the constitution;

- Benefits of public officials: adopt a law for declaring benefits of public officials.

- Participation and protection of civil liberties: involve citizens in policy formulation and governance, including protecting civil liberties;

- In addition to meeting the aforementioned criteria, countries wishing to join the Open Government Partnership are subject to two additional measures:

    - The level of oversight over non-governmental organizations when entering and exiting public life;
    - Extent of government control over non-governmental organizations.

3. *After joining the Open Government Partnership*

Countries that join the initiative commit to preparing a national open government action plan every two years, which stipulates a number of projects that support the principles of open government. The action plans are prepared and executed in collaboration between governmental and non-governmental agencies, in a framework of public consultations. The action plans involve projects related to promoting open government, and rely on information and communications technology. Examples include supporting transparency by disseminating open data; enacting laws on the right to access information; strengthening integrity in the public sector and fighting corruption; improving publicly managed administrative services; and increasing citizen engagement by establishing a framework to encourage public consultations and receive petitions and complaints.

Each member State in the initiative must launch a dialogue between the Government and non-governmental organizations on the national Open Government Partnership programme, to be organized periodically and preferably monthly. This forum is coordinated by a national leadership committee

composed equally of representatives of government agencies and representatives of non-governmental agencies (non-governmental organizations, academics, the private sector). At the sessions, participants follow up on the implementation of national action plans related to the Open Government Partnership, discuss various evaluation reports, and approve new action plans. The Executive Office of the Open Government Partnership monitors the various action plans of its member States, issues semi-interim and final evaluation reports on these plans, and publishes them after they are presented to the public for consultation.

The phase after joining the Open Government Partnership is the most challenging and most rewarding. Members develop programmes and projects with a reform dimension, which respond to the needs of society and support the principles of open government.

B. Open data

Open Knowledge International defines the word 'open' when referring to information as information that anyone can access, use, modify and freely share with anyone for any purpose (subject, at most, to requirements that preserve provenance and openness).[5] This institution also defines open government data as "data produced or commissioned by government or government controlled entities", which "can be freely used, reused and redistributed by anyone".[6]

Open Data Charter defines open data as "digital data that is made available with the technical and legal characteristics necessary for it to be freely used, reused, and redistributed by anyone, anytime, anywhere".[7]

Open government data policies support transparency, accountability and added value, by making government data accessible to everyone. Governmental institutions, which produce huge amounts of data and information, can become more transparent and accountable by making their data public. They can also provide better services to citizens by encouraging the use of this information and by re-using and distributing it freely, which helps create startups and provide new job opportunities.

The concept of open data emerged recently (compared with the concepts of transparency and openness) in response to citizens' requests to access information collected by Governments on various sectors. Advancements in information and communications technology have facilitated the collection, storage and dissemination of data. The first open data policy was established in 2009. Since then, hundreds of initiatives have been implemented worldwide at the national, subnational and local levels, in addition to initiatives by international organizations such as the World Bank, the United Nations and the European Union.

Open data and open government are two related but different concepts. Open data can be an essential part of a broader programme of open government. By publishing government data in digital

[5] The Open Definition project. Available at https://opendefinition.org (accessed on 6 April 2020).

[6] Open Government Data website. Available at https://opengovernmentdata.org (accessed on 6 April 2020).

[7] Open Data Charter website. Available at https://opendatacharter.net (accessed on 6 April 2020).

form and enabling their reuse, these data can support transparency, cooperation and participation, which are fundamental principles of open government.

Principles and objectives of open data

The Open Data Charter sets out six open data principles as a basis for accessing, disseminating and using data.[8] These principles, drawn from the Open Definition,[9] require that data meet the following criteria:

- Open by default: public sector data is by default open, which means that they are available to everyone. Exceptions can be made for some types of data, such as security and personal data;
- Available in a timely and comprehensive manner: information should be disseminated quickly and in a comprehensive manner, so that data are presented in their original and unmodified form;
- Accessible and usable: files open in a machine-readable format, and are easy to access, free of charge, and subject to an open license;
- Comparable and interoperable by adopting common data standards;
- Used to strengthen governance and citizen participation: by increasing transparency and government accountability;
- Employed for comprehensive economic development and job creation by establishing innovative and value-added services.

The following are the main objectives for developing open data projects:

- **Increasing transparency and accountability:** The right to access government data is determined by freedom of information laws, but government data consumption and reuse are facilitated through open data. Dissemination of open government data enables collaboration between Governments, citizens, and non-governmental organizations to formulate better policies and make informed decisions through innovative ideas can generate social and economic benefits;
- **Ensuring economic value:** requires the use of open data to develop value-added services, especially for the transport, agriculture and health sectors. Today, economic impact has become the main objective behind the development of open government data strategies and policies, given the amount of employment opportunities they can generate;

[8] Ibid.

[9] The Open Definition project. Available at https://opendefinition.org (accessed on 6 April 2020).

- Improving public services: through direct investment in open government data or through the use of applications developed using open data. Quality open data is essential for developing better services for citizens;

- Promoting marketing value: data dissemination by local groups and cities helps attract visitors and investors, indicates good governance and social cohesion, and stimulates investors, business prosperity and job creation.

II. Legislation on Open Government and Open Data

Such legislation promotes the principles of open government, namely participation, transparency and accountability, and the opening and dissemination of government data for reuse by the public. In an unpublished study, Toby Mandal, a Canadian expert on open government, lists 44 laws on establishing open government and disseminated government data. These laws are diverse and cover many areas, such as access to information, confidentiality of information, press and publication, events, economic crimes, anti-corruption, civil, criminal, military and security issues, cybercrime, public and commercial security, copyright, financial and banking issues, associations, personal status, religious issues, elections, statistics and personal data protection.

The present study focuses on laws that have a significant impact on the principles of open government, especially transparency and the right to access open information and data. It also considers legislation on participation and accountability.

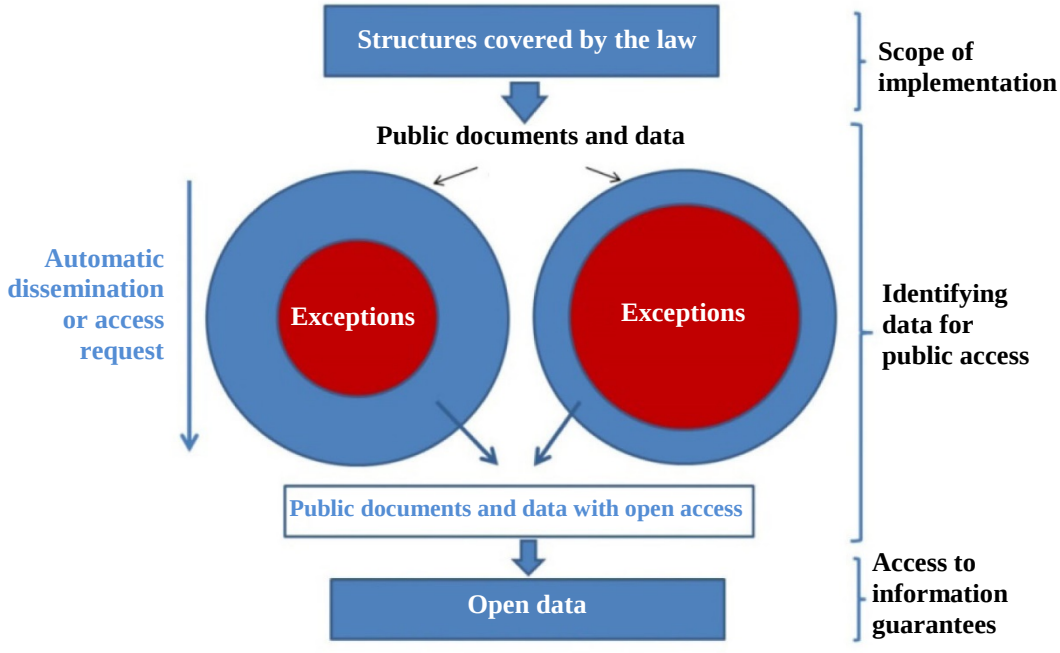
A. Legislation on the right to access information

Laws on the right to access information are an essential part of open government legislation, as they give citizens the right to access documents and information on public issues, the operation of public utilities, and decision-making processes. They support transparency in government action by requiring public institutions to automatically publish documents and data, thus facilitating oversight of administrative performance, which assists in combatting various forms of corruption, including bribery and nepotism, within the public sector. Access to information laws are the cornerstone of governance system based on transparency, accountability and open government system, which may explain recent demands for enacting such laws in countries that lack them.

The importance of the right to access information is highlighted by the number of countries that have enacted these laws, reaching 124 in 2019 compared with 13 in 1990. The Open Government Partnership indirectly requires that countries wishing to become members adopt a law on the right to access information, in the absence of such a law, as countries without these laws cannot reach a high enough score to join the Partnership.

Laws on the right to access information differ between countries in terms of degree of openness and the bodies responsible for disclosure and access to information guarantees, which prompted international institutions to issue methodologies for evaluating and classifying such laws. Given that the degree of openness in these laws is closely related to the political, cultural and security specificities of a country, many methodologies in the field of open government do not attach importance to the provisions contained in these laws, but rather focus on the mandatory enactment of such laws. For example, the Open Government Partnership's membership criteria do not cover the type of legislation on the right to access information, but only whether such laws exist.

Figure 2. Laws on the right to access information



Source: Compiled by ESCWA.

1. *Historical overview of the right to access information*

Article 19 of the 1948 Universal Declaration of Human upholds the right to access information: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers". Although this right is not explicitly mentioned in the text, article 19 is considered the first step towards cementing this right. Article 19 of the 1966 International Covenant on Civil and Political Rights stipulates the following: "Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice". In 1993, the United Nations Commission on Human Rights created the post of Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. In its 1998 annual report, it states that the right to request, obtain and disseminate information requires States to ensure access to information.

In 1766, Sweden became the first country globally to enact a law guaranteeing the right to access administrative information. Finland followed in 1951, making the United States of America the third country to enact such laws in 1966, followed by France in 1978.

2. *Principles to be observed in laws on the right to access information*

Enacting laws on the right to access information requires the application of several basic principles that must be reflected in the provisions of the laws, including respecting the principle of

maximum disclosure, restricting exceptions to this principle, not exempting any public institution from the duty to disclose, facilitating requests for and access to information, and upholding the right to appeal and litigate to achieve access.

Since 1999, Article 19, a British human rights organization, has developed nine principles relating to the right to access government information.[10] The organization believes that those principles should be taken into account in national legislation to maximize openness of information. These principles were adopted by the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression in a report he submitted to the United Nations Commission on Human Rights in 2000. These nine principles are:

(a) **Maximum disclosure:** Freedom of information legislation should be guided by the principle of maximum disclosure, meaning that all information held by public bodies should be subject to disclosure, with very limited exceptions; that everyone within the State's borders has the right to access this information; and that persons requesting this information are not required to justify their interest therein. 'Information' and 'public bodies' should be defined broadly to cover these requirements. The law should provide that obstruction of access to or the wilful destruction of records is a criminal offence;

(b) **Obligation to publish:** Public institutions should be under an obligation to publish key information. The right to access information not only means that public bodies should accede to requests for information, but also that they should publish and disseminate widely documents of significant public interest. The law on access to information should establish both a general obligation to publish and key categories of information that must be published;

(c) **Promotion of open government:** Public bodies must actively promote open government, by informing citizens of their rights and promoting a culture of openness within government departments. The law should require that adequate resources and attention are devoted to promoting access to information, and should commission a special information and awareness-raising mechanism and provide it with the necessary resources. This mechanism could also be responsible for considering requests to access information. The law should provide for a number of mechanisms to address the problem of a culture of secrecy within government by providing training to government officials on open information;

(d) **Limited scope of exceptions:** Exceptions should be clearly and narrowly drawn and subject to strict 'harm' and 'public interest' tests. A list of exceptions can be included in the law (for example: breach of privacy, threats to national security or the public interest, commercial interests). A refusal to disclose information is not justified unless the public authority can show that the information meets a strict three-part test:

(1) The information must relate to a legitimate aim listed in the law;
(2) Disclosure must threaten to cause substantial harm to that aim;
(3) The harm to the aim must be greater than the public interest in having the information.

[10] Article 19 website. Available at https://www.article19.org/data/files/pdfs/standards/righttoknow.pdf (accessed on 6 April 2020).

(e) **Processes to facilitate access:** Requests for information should be processed rapidly and fairly and an independent review of any refusals should be available. A process for deciding upon requests for information should be specified at three different levels: within the public body; appeals to an independent administrative body; and appeals to the courts. Provision should be made to ensure full access to information for persons with special needs. All public bodies should facilitate access to information and designate an individual responsible for processing requests within strict time limits. Any refusals must be accompanied by substantive written reasons;

(f) **Costs:** Individuals should not be deterred from making requests for information by excessive costs. The cost of gaining access to information held by public bodies should not be so high as to deter potential applicants. The fees for responding to requests for access to information should, at the most, reflect the costs of providing such information;

(g) **Open meetings:** Meetings of governing bodies should be open to the public, especially those of elected bodies responsible for taking decisions regarding requests to access information. The public must be informed of the dates of those meetings;

(h) **Disclosure takes precedence:** Laws which are inconsistent with the principle of maximum disclosure should be amended or repealed. The law on freedom of information should require that other legislation be interpreted, as far as possible, in a manner consistent with its provisions. Where this is not possible, other legislation dealing with publicly-held information should be subject to the principles underlying the freedom of information legislation;

(i) **Protection for potential whistleblowers:** Individuals should be protected from any legal, administrative or employment-related sanctions for releasing information on wrongdoing, including corruption, crime or administrative errors.

Laws on the right to access information differ in their compatibility with these principles, since most laws globally, especially old ones, do not fully comply with these principles, which requires revision or enactment of new laws. Despite the low quality of such laws in a number of ancient democracies, the entrenched culture of the right to access government information in these countries, and the development of access practices, make them uninterested in amending their laws to suit current standards.

3. *Laws on accessing information to ensure transparency and anti-corruption*

Corruption in public institutions remains the biggest obstacle to good governance and open government. Corruption erodes trust between the Government and citizens, encourages non-investment, and contributes to low growth. Fighting corruption requires mechanisms to support the transparency and accountability of public institutions, by providing citizens with ways to hold them accountable and to access their information.

Laws on access to information are one of the most efficient mechanisms for citizens to hold Government accountable and access data and documents. They are therefore an effective tool to detect corruption and bribery. An example of this is public procurement files that may involve fraud in the choice of provider or inconsistencies with regulations, which may indicate corruption. Moreover, detecting administrative breaches by accessing information related to the provision of administrative

services can be an indication of bribery and corruption. These cases may remain undetected in the absence of a mechanism that allows public access to information.

Fields in which there are exceptions to laws on access to information remain subject to corruption, which explains the inclusion of provisions that allow the disclosure of information for the public interest, even in areas listed as exceptions. Such laws help eradicate the culture of secrecy within Government thereby uprooting corruption, and pave the way for more reforms, accountability and transparency in governments work.

Optimizing laws of access to information is predicated on their effective application, which requires government will and commitment. Laws are not the only way to eliminate corruption: they must be accompanied by other measures, such as simplifying and digitizing administrative methods, raising awareness among government employees and promoting integrity, until all outlets for corruption are eliminated.

4. *Criteria for evaluating laws on access to information*

Drafting legal texts on the right to access information requires referral to references that assess the alignment of such texts with international standards. In this context, a number of methodologies have been developed that can be used to enact laws on access to information, according to country specificities.

Box 1 sets out the RTI Rating[11] methodology for assessing laws on the right to access information, and related standards and indicators. It was developed by the Centre For Law and Democracy in Canada.[12]

Box 1. Methodology for evaluating laws of access to information

The Centre for Law and Democracy and Access Info developed a methodology for evaluating laws on the right to access information, based on -seven criteria and 61 indicators. These indicators measure the efficiency of laws on access to information, and are used as references for drafting new laws or revising existing laws.

Moreover, these two bodies developed a methodology for assessing all laws globally (RTI Rating) based on these indicators, and established an international classification of these laws. This numerical assessment is also used as a reference for identifying the specifications of laws on the right to access information.

The following are the criteria and indicators:

1. Right to access information

- A constitutional right;
- Provides access to all information held by public institutions, with some exceptions;
- Lists the positives of accessing information and recalls related principles.

[11] www.rti-rating.org.

[12] www.law-democracy.org/live.

2. Scope of law enforcement

- Everyone has the right to apply for information;
- This right applies to all government data, regardless of who produced it;
- The right to request specific information or documents;
- This right applies to all structures and senior officials;
- The law applies to the legislator;
- The law applies to judicial institutions;
- The law applies to public institutions;
- This right applies to independent and constitutional bodies;
- This right applies to private institutions that provide a public service or receive public money.

3. Procedures for requesting information

- Requesters are not required to justify their request;
- Requesters are not required to provide their name or address;
- There are clear and relatively simple procedures for making requests, with the option to submit requests by email;
- Assist requesters formulate and inform them when there are problems with their request;
- Assist requesters with special needs;
- Provide a receipt to requesters;
- Inform requesters if the information required is unavailable, and refer them to the bodies that own it;
- Comply with requesters' preferences regarding how they access information;
- Respond to requests for information as soon as possible;
- Identify clear response times and deadlines;
- Set clear limits on timeline extensions and provide reasons for the extension;
- Requests are free of charge;
- Set clear rules relating to access fees and exempt the first 20 pages from fees;
- Provide fee waivers for impecunious requesters;
- No limitations on reuse of information, except in the case of information subject to intellectual property laws.

4. Exceptions and refusals

- Laws on access to information trump other laws that restrict access to information;
- Exceptions must be in line with international standards;
- A harm test applies to all exceptions to assess the risk of accessing information;
- The public interest is given precedence over all exceptions;
- Information is released as soon as an exception ceases to apply;
- Consult with third parties who provided information;
- When only part of a record is covered by an exception, the remainder must be disclosed;
- Inform requestors of the reasons for the refusal.

5. Appeals

- Requesters have the right to lodge an appeal with an independent administrative oversight body if the request is refused, with specific deadlines;
- The possibility of challenging the refusal through an independent body;
- Members of an independent body have immunity from expulsion;
- The budget of the independent body is determined and monitored by parliament;
- Prohibitions on individuals with strong political connections from being appointed to this body and requirements of professional expertise;
- The authority has access to classified documents;
- Decisions of the independent body are binding;
- The independent body has the right to declassify information;
- The requestor can appeal the decision of the independent body to the judiciary;
- Appeals to the independent body are free of charge;
- Grounds for an external appeal are broad;
- Clear procedures, including timelines, are in place for dealing with external appeals;
- Decisions of the independent body are supported by evidence;
- The independent body has the power to impose structural measures on public institutions.

6. Penalties and guarantees

- Sanctions may be imposed on those who wilfully act to undermine the right to information, including through the unauthorised destruction of information;
- Sanctions against institutions that systematically fail to disclose information;
- Members of the independent body are granted legal immunity for acts undertaken in good faith;
- Legal protections against imposing sanctions on those who, in good faith, release information which discloses wrongdoing.

7. Promoting the right to access information

- Appoint officials with dedicated responsibilities for ensuring that public institutions comply with their information disclosure obligations.;
- Mandate a central body to promote the right to access information.
- Provisions of education and training and dissemination of evidence on access to information;
- Establish standards regarding the management of records;
- Public authorities are required to create and update lists or registers of the documents in their possession;
- Training programmes for officials on access to information;
- Public institutions prepare annual reports with statistics on the status of access to information;
- Prepare an annual report to be submitted to the legislature.

The assessment methodology assigns weighting factors for each indicator according to its presence in laws on the right to access information. The total is 150 points, which is the maximum number of points that can be scored by any law on the right to access information.

Source: RTI Rating, https://www.rti-rating.org/country-data/by-indicator.

Assessment indicators can be included in the provisions of laws on the right to access information. When drafting such laws, it is useful to use the indicators to identify provisions and include as many indicators as possible to guarantee the value of the law. Today, the Right to Information Act in Pakistan is considered the best globally, as the country scores a total of 139 out of 150 points, according to this assessment.

5. *Right to access information in the Arab region*

Six Arab countries issued laws on the right to access information. In 2007, Jordan enacted its law on access to information, followed by Tunisia in 2011 and Yemen in 2012. The number of Arab countries that have passed laws on access to information remains small compared with other regions.

Table 1 shows Arab countries that have issued laws on the right to access information, the year of issuance, and the total points scored under the RTI Rating.

Table 1. Arab countries that have issued laws on the right to access information

Countries	Stipulated in constitution	Stipulated in law	Year of issuance	2019 RTI Rating
Jordan	Yes	Yes	2007	56
Tunisia	Yes	Yes	2011	120
Yemen	No	Yes	2012	103
Sudan	No	Yes	2015	64
Lebanon	No	Yes	2017	70
Morocco	Yes	Yes	2018	73

Source: RTI Rating.

According to the RTI Rating, Tunisian law is the best in the Arab world with 120 points. This law ranks twelfth out of 124 laws worldwide, followed by the Yemeni law with 103 points.

Box 2. Exceptions to the right to access information according to Tunisian law

Chapter 4
Exceptions to the right to access information

Article 24: The body concerned can refuse access to information only in cases of threats to national security, defence, international relations or the protection of individuals' private life, personal data or intellectual property.

These are not absolute exceptions to the right to access to information. They are subject to a damage assessment to consider whether the resulting harm would be severe, immediately or in the future. Public interest is also a factor when deciding whether or not to provide information. A balance shall be struck between the interests to be protected and the purpose of accessing information.

If refused, the applicant shall be notified with a reasoned response. The refusal ends with the expiration of the reasons expressed in the response.

Article 25: Access to information does not include data related to the identity of persons who provided information with the intention of reporting violations or corruption.

Article 26: The exceptions provided in article 24 of the present law do not apply to the following:

- Information necessary for uncovering, investigating or tracking perpetrators of gross human rights violations or war crimes, unless it affects State interests;
- When the public interest must prevail over the harm that may be caused to the protected interests owing to a serious threat to health, safety or the environment, or the occurrence of a criminal act.

Article 27: If the required information is partly covered by the exceptions stipulated in articles 24 and 25 of the present law, it can only be accessed after the information under the exception is withheld, whenever possible.

Article 28: Information that cannot be accessed under article 24 of the present law shall be accessible according to the terms and conditions stipulated in the legislation related to archiving.

Source: Organic law No. 22 of 24 March 2016 on the right to access information.

Organic law No. 22 of 24 March 2016 on the right to access information is one of the most important laws passed in recent years in Tunisia, along with a number of other laws related to the promotion of good governance and open government. These laws include law No. 10 of 7 March 2017 on reporting corruption and protecting whistleblowers; law No. 46 of 1 August 2018 on declaring gains and interests and combating unjust enrichment and conflicts of interest.

The National Authority for Access to Information was established in Tunisia in August 2017. According to the law, its functions include deciding on access to information cases, disseminating a culture of access to information, and preparing necessary evidence to implement this right. Since 2017, the Authority has received over 1,000 requests to challenge the decisions of administrative bodies regarding requests for access to information. It has ruled on 656 of those cases, with 44 per cent of its

rulings in favour of the requestor, partially or completely. This large number of appeals shows the considerable recourse to the law to obtain information or documents, and highlights the credibility of this law that has greatly contributed to supporting trust in the Tunisian system of governance. It has also helped many parties access important information on corruption cases, restore rights or raise public awareness. The biggest challenge in this field is entrenching a culture of open information within public institutions through automatic publication and rapid responses to requests for information.

The absence of provisions on the right to reuse government data must be rectified in the Tunisian law on the right to access information, so as to complete the legislative framework related to the right to access information and open data.

The level of application of laws on the right to access information varies in other Arab countries that have passed them, depending on various factors. In Jordan, law No. 47 of 2007 on guaranteeing the right to information stipulates the formation of an information council chaired by the Minister of Culture, comprising directors of government institutions. The council's responsibilities include ensuring the provision of information to requestors, and considering complaints submitted by requestors. Since 2008, the council has received 50 complaints from requestors whose applications were rejected.[13] Jordanian law has been enhanced by a 2019 draft policy on classifying and managing government data in Jordan, which was presented for public consultation.[14]

In Yemen, the law excludes data related to military strategies, weapons and military operations, classified data related to the State's foreign policies or classified information exchanged with other countries, and information that could cause serious harm if disclosed.[15] The law provides for the establishment of an Office of the Commissioner-General for Information, responsible for organizing related programmes and raising public awareness. It is a recourse for those whose requests for information have been rejected. However, law enforcement remains limited owing to the current situation in the country.

In Lebanon, a law was passed in 2017 stipulating that the National Anti-Corruption Commission should consider complaints from those whose applications for information have been rejected.[16] The applicant must submit a written request to the Authority, which assigns staff members to consider requests for information from institutions, and provide a response within 15 days. The application of the law is still limited owing to a lack of implementation decrees.

In 2018, Morocco enacted a law excluding data that could pose a national security risk, such as financial and monetary policies, foreign relations, industrial property rights and copyrights.[17] Information can be obtained by submitting an application to the head of the institution concerned, whether in writing or electronically. The law also provides for the establishment of a "right to information committee" under the Prime Minister, tasked with ensuring the application of the law and

[13] Yahya Shuqeir, Arab Reporters for Investigate Journalism, Access to Information in the Arab World.

[14] www.modee.gov.jo.

[15] Law No. 13 of 2012 on the right to access information, Yemen.

[16] Law No. 28 of 2017, Lebanon.

[17] Law No. 13 of 2018, Morocco.

handling complaints. Table 2 compares legal texts on the right to access information and their application in Arab countries.

Table 2. Comparison of legal texts on the right to access information and their application in Arab countries

	Jordan	Yemen	Tunisia	Sudan	Lebanon	Morocco
Automatic dissemination	No	Yes	Yes	Limited	Yes	Yes
Paper or electronic request	Paper	Paper	Paper and electronic	Paper	Paper	Paper and electronic
Reason required to request information	Yes	No	No	No	No	For legitimate purposes
Presence of an independent complaints authority	Information council	Office of the Commissioner-General for Information	National Authority for Access to Information	-	National Anti-Corruption Commission	Right to information committee
Decisions of the complaints authority are binding	Non-binding	Non-binding	Binding	Non-binding	Binding	-
Timeline for responding to requests	30 days	15 days	20 days	15 days	15 days	20 days
Penalties for employees who deliberately do not respond to requests	None	Fine or prison	Fine and disciplinary measures	Prison	None	Disciplinary measures
Affordable fee for accessing information	Yes	Yes	Yes	Yes	Yes	Yes
Possibility to appeal refusals in a court	Administrative court	Regular courts	Administrative court	Administrative court	Administrative court	Administrative court
Law oversight body publishes reports on its work	No	Yes	Yes	Yes	Yes	Yes

Source: Yahya Shuqeir, Arab Reporters for Investigate Journalism, Access to Information in the Arab World.

6. *Comparison of laws on the right to access information*

Legislation on the right to access information differs between countries according to their social, economic and political specificities, and depending on how recently the law was enacted. Laws issued in the past two decades contain more sophisticated provisions than previous laws, and are aligned with modern standards for laws on the right to access information, especially in terms of information request procedures, exceptions and guarantees to obtain information. An example of this is Central European countries that are members of the European Union, which have passed laws on access to information following their independence and before they joined the European Union. Slovenia issued a law on accessing government data in 2003, and revised it in 2014. It is currently ranked fifth globally in the RTI Rating with 129 points. Slovenian and Serbian laws are the best in Europe. The Slovenian law is

distinguished in terms of procedures for requesting information and guarantees for obtaining it, and assesses exceptions to the law differently. Table 3 sets out key provisions of the Slovenia law on the right to access information.

Table 3. Keys provisions of the Slovenia law on the right to access information

Topic	Provisions
Scope of application	• Bodies concerned: State institutions, local government institutions, public institutions, public funds and public law bodies, those with public influence, and public service providers; • Non-citizens and institutions can also apply to access information. Government data held by private sector companies are covered by law.
Process for requesting information	• The applicant is not obligated to justify his request; • The applicant identifies the most appropriate method for obtaining information; • No fees are charged for submitting a request to access information; • Fees equivalent to the cost of reproducing the information may be charged; • Fees may be charged in case of information re-use; • Response to access requests must be provided within 20 days.
Exceptions and refusals	• Exceptions: o Information classified as confidential according to the Classified Information Act; o Business information classified as confidential according to the Corporate Governance Code; o Personal data in accordance with the Personal Data Protection Act and the National Statistics Act; o Information affecting tax confidentiality in accordance with the tax law; o Information whose disclosure disrupts the judicial process; o Information whose disclosure disrupts administrative procedures; o information under consideration whose contents may be misunderstood; o Information whose disclosure may disrupt by the operations of facilities concerned; • Not giving precedence to the public interest over all exceptions (e.g. classified information according to the Classified Information Act); • Not disclosing information even when the original reasons for withholding it are no longer valid.
Complaints and appeals	• Appeals are filed with the Commissioner for access to public information, with a 15 day-day response deadline; • Appeals are free of charge and do not require legal assistance; • The Commissioner is independent, and elected by parliament. The Commissioner's work is regulated by a separate law. The Commissioner also fulfils the role of Commissioner for the protection of personal data; • Administrative litigation regarding the decisions of the Commissioner is possible.

Topic	Provisions
Sanctions and protections	• Fines are levied against those who commit the following acts: o Destroy information to not disclose it; o Fail to provide supporting evidence for a complaint lodged with the Commissioner for access to public information; o Failure to provide students with information, despite the Commissioner's decision to allow access to government data; o Failure to submit an annual report on the implementation of the Access to Public Information Act within the deadlines specified in the law; • Failure to establish judicial immunity for the Commissioner and his assistants; • Failure to establish judicial immunity for those who disclose, in good faith, false information.
Promoting the right to access information	• Legal bodies appoint one or more employees to uphold the right to access information; • The Ministry of Public Administration is the body charged with promoting the right to access information and raising awareness in this regard; • The Government is tasked with preparing an annual report on the implementation of the law, which is presented to parliament.

Source: RTI Rating, www.rti-rating.org/country-detail/?country=Slovenia.

B. Legislative framework for open data

The legislative framework for open data includes legal aspects related to the citizens' right to access and use government data, and the categories of data included in information automatically published by public institutions. This framework also includes the right to reuse and distribute data, grant a license for reuse, publication exceptions and the protection of personal data, among others. It covers organizational aspects related to managing government open data programmes, developing open data portals, metadata, data quality, free government data or related fees, and the governance of open data programmes, among other aspects.

In general, the legal aspects of open data are included in the law on the right to access information, which includes provisions relating to the automatic dissemination of information, the right to reuse government data, and the need to publish a license for reuse. Exceptions listed in the law on the right to access information apply to open data; it is not possible to publish government data included in those exceptions. Open government data may be covered by a law that contains provisions on its reuse, the necessity to publish a license, and other regulatory provisions such as programme governance and free open data.

If the legal aspects of open data are adopted in the law on the right to access information, the organizational aspects of open data are usually included in this law in the form of regulatory instructions or orders published in the Official Gazette. If the law is adopted without provisions related to the reuse of information, it must either be revised to add those provisions, or a special reuse law should be issued that is consistent with the right to access information.

1. *Necessity of developing a law guaranteeing the right to access information*

It is not possible to talk about open data policies in the absence of a law guaranteeing the right to access information and allowing its reuse. These laws are the legal umbrella to opening government data, as they provide a legal framework for making data publicly available for use. Government data that are legally classified under 'automatic publishing' must be published. Government data that do not fall within the exceptions stipulated in the law on accessing information are legally available to the public, and therefore can be requested and obtained legally from public institutions. The institutions to which the law applies are also concerned with the publication of open data.

2. *Right to reuse data*

The main aim of obtaining open data is to reuse it to create added value. Legal provisions must therefore be included that allow the reuse of open government data without restrictions, except in cases of intellectual property. Legal provisions have to be included that require a reuse license for every data set that is published to protects the rights of parties that publish or reuse data.

3. *Open data reuse licences*

Accessing and downloading information or data does not automatically confer the right to reuse them, since this requires a license from the owner, even if the owner publishes them. Data published without a license cannot even be viewed, and cannot be shared or reused. Accordingly, the license attached to the published data must be viewed to know the rights related to it. Open data licenses define the legal aspects related to data reuse, as follows:

- Rights to access information;
- Right to use information;
- Right to share and redistribute information.

Open data licenses cover reuse aspects only, and do not cover publishing aspects such as protection of personal data or copyright. It is not possible to reuse data without a license, therefore eliminating the positive effects of open data. An open data reuse license can restrict the following:

- Republishing and adding value to data;
- Posting sections of the data;
- Developing data derivatives;
- Making profit through the use of data;
- Republishing the data for a fee.

The license may include the following restrictions:

- Attribution (BY);
- Share alike (SA);
- Non-commercial use (NC);
- No derivatives (ND).

A public domain licence eliminates any restrictions on the reuse of open data. An open license places limited restrictions on the use of data, as follows:

- Attribution: reference to product and date;
- Using the same license.

In the context of developing open government data policies, one or more open government data licenses are being developed for approval by government agencies. The obligation to adopt open data licenses developed nationally can be included in the regulatory frameworks of open data. It is recommended that these licenses be simplified, easy to understand, open to the greatest possible extent, few in number, and conform to global licence specifications.

Creative Commons (CC) and Open Data Commons (ODC) have released open licenses. Many countries and organizations adopt these licenses when publishing their data. Table 4 sets out various open licenses and their limitations.

Table 4. Open licences

Licence	Type	Public domain	Attribution	Share alike	Non-commercial	Database only	No derivative
CC-0	Public Domain	*					
ODC-PDDL	Public Domain Dedication and License	*				*	
CC-BY	Attribution License		*				
ODC-BY	Attribution License		*			*	
CC-BY-SA	Attribution-ShareAlike		*	*			
ODC-ODbL	Open Database License		*	*		*	
CC BY-NC	Attribution-NonCommercial		*		*		
CC BY-ND	Attribution-NoDerivs		*				*
CC BY-NC-SA	Attribution-NonCommercial-ShareAlike		*	*	*		
CC BY-NC-ND	Attribution-NonCommercial-NoDerivs		*		*		*

Source: Creative Commons website, https://creativecommons.org/licenses; data.world website, https://data.world/license-help; Open Data Commons website, https://opendatacommons.org/licenses.

4. *Organizational aspects of open data*

The organizational aspects of open data include a methodology for inventorying and disseminating government data, governance of government open data programmes, managing the national open data portal and connecting with other open data portals, description of data and description components, quality and type of data, programme evaluation and follow-up, free data or fees, available licenses, and personal data.

Table 5. Comparison of regulatory aspects of open data in several countries

Components	Country
Open data portal	United Kingdom, Kenya, India, Tanzania, Ethiopia
Licences	United Kingdom, United States, Denmark, Philippines, Kenya, Ethiopia
Adopting a five-level evaluation	United Kingdom, Philippines, Qatar
Free of charge	United States, Denmark, Kenya, Ethiopia
Fees	United Kingdom (limited), Qatar, France (limited)
Governance system	United Kingdom, United States, Australia, India, Rwanda, Tanzania, Ethiopia
Personal data protection	United Kingdom, United States, Japan, Australia, France
Publishing priorities	United Kingdom, United States, Philippines, India, Denmark, Japan, Australia
Monitoring and evaluation plan	United Kingdom, United States, Ethiopia
Participatory mechanism	United Kingdom (forum), United States, Rwanda, Qatar (forum), Ethiopia
Open data (by default)	United Kingdom, United States, Ethiopia, Rwanda, South Africa, Tanzania
Exceptions	United Kingdom (law enforcement), United States (against competition), Tanzania (sectors)

Source: SBC4D website, sbc4d.com.

The organizational aspects of open data usually take the form of government or presidential orders (instructions), and are published in the Official Gazette (for example, Mexico,[18] Brazil[19]). Regulatory aspects may be published within an open data law that includes the right to reuse (for example, South Korea,[20] the United Arab Emirates - Dubai[21]).

[18] Open Government Data Review of Mexico, Organization of Economic Cooperation and Development, P66, 2016.

[19] Portal Brasileiro de dados abertos. Availbale from http://dados.gov.br/pagina/instrucao-normativa-da-inda (accessed on 6 April 2020).

[20] Act on promotion of the provision and use of public data. Available at http://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=30365&type=part&key=4 (accessed on 6 April 2020).

[21] Law No. 26 of 2015 on regulating data dissemination and exchange in the Emirate of Dubai. Available at https://www.smartdubai.ae/docs/default-source/dubai-data/data-dissemination-and-exchange-in-the-emirate-of-dubai-law_2015.pdf?sfvrsn=46ac2296_6#:~:text=An%20electronic%20or%20paper%2Dbased,3%20of%2010%20the%20Electronic (accessed on 6 April 2020).

Box 3. Open data law of Dubai

The United Arab Emirates issued law No. 26 of 16 October 2015 on regulating data dissemination and exchange in the Emirate of Dubai. The law aims to optimize the use of data available to data providers, enhance transparency and establish the rules of governance of data dissemination and exchange, and provide necessary data to non-governmental bodies, with a view to supporting development and economic plans in the emirate.

The law regulates government data, which it categorizes as either open data, which are data that are released to the public; or shared data that is shared only between government agencies. The provisions of this law apply to the following:

1. Federal government agencies with any data related to the emirate.
2. Local government entities.
3. Persons who produce, own, disseminate, or exchange any Data relating to the Emirate, and who are determined by the Competent Entity whether they are individuals, establishments, or companies in the Emirate, including Special Development Zones and free zones, such as the Dubai International Financial Centre.

The implementation of law shall be supervised by a competent entity to be determined in accordance with a legislative text. Its tasks include identifying data providers from government agencies; monitoring data providers' compliance with policies adopted for data dissemination and exchange; investigating complaints and violations regarding data providers adherence to the law; and other coordination and control tasks regarding opening data.

The law includes provisions related to the electronic platform used for data dissemination and exchange and related infrastructure, and other provisions that require local government agencies to classify their data according to a guide, follow policies approved by the competent entity to disseminate and exchange open data, and ensure the quality of their data.

This law is considered a unique model in the field of open data legislation in the Arab region. Failure to address issues related to the reuse of published data and reuse licenses is a major gap in this law, which may hinder the optimal use of disseminated data.

Source: Law No. 26 of 2015 on regulating data dissemination and exchange in the Emirate of Dubai.

III. Legislation on Open Government, Open Data, and the Right to Access Information

Studies about laws on the right to access information have shown that the provisions of many other laws may overlap with this right, and therefore these laws must be reviewed to ensure that the law on the right to access information takes precedence over other laws. Numerous laws could be related to the right to access information, and may cover many areas such as access to information, confidentiality of information, press and publication, events, economic crimes, anti-corruption, civil, criminal, military and security issues, cybercrime and public security, trade, copyright, finance, banking, associations, personal, religious and electoral status, statistics, personal data protection and public services.

The present section addresses various legislation related to open government and the right to access information and open data. These laws are divided into the following two categories:

- Laws that limit the right of access by narrowing the scope of access. They largely cover areas related to exceptions contained in laws on the right to access information;
- Laws that support the right of access, and thus provide mechanisms to access information in specific sectors.

A. Laws limiting the right to access information

All laws on the right to access information contain a limited number of exceptions related to sensitive issues, such as public safety, State security and foreign relations, or to uphold individual rights such as protecting personal data or intellectual property rights. These areas and rights are usually regulated by laws issued prior to laws on the right to access information, and therefore they may overlap. The following sections review some of these laws.

1. *Laws protecting personal data and private life*

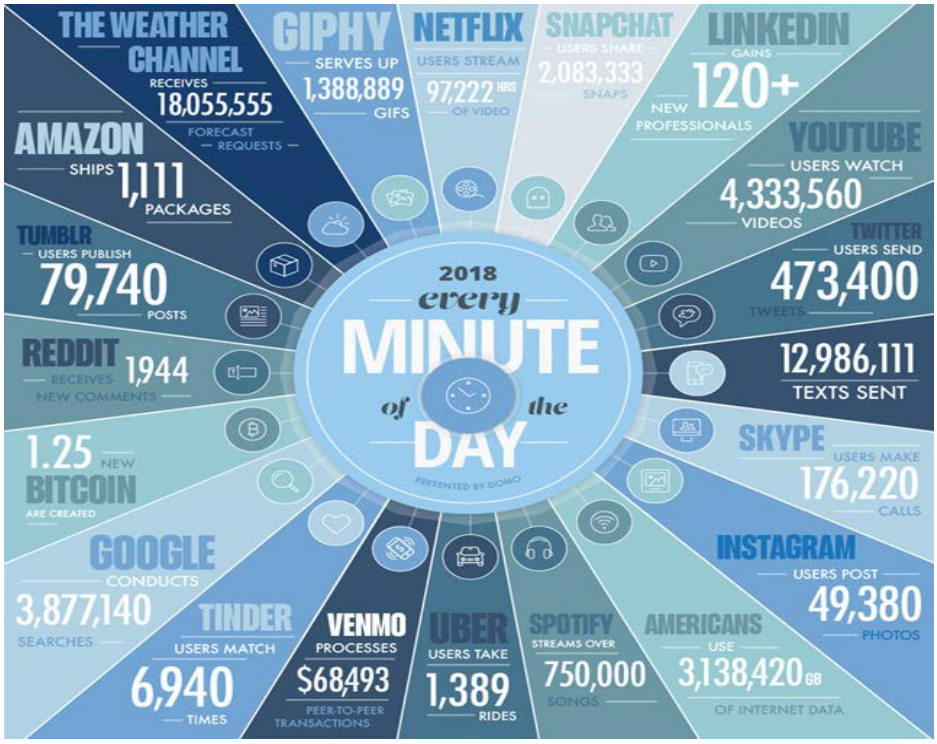
The rapid advancement of modern technologies has increased the risks related to personal data circulation, especially in view of the widespread use of social networks, mobile services and Internet applications, which expose personal data to theft and unauthorised use, and in turn may harm the private life of individuals.

The right to protect private life is one of the most important human rights. Article 12 of the Universal Declaration of Human Rights stipulates that all people have the right to protect their private life.[22] Personal data is the main focus of this protection, as it is a key component in modern digital economic systems.

In recent years, the world has witnessed a considerable increase in data generation and circulation, especially personal data, as a result of considerable demand for new applications where large amounts of personal data are stored in various forms, including geographic information, videos, pictures, messages and associated personal data. Figure 3 highlights the extent of this data generation.

[22] www.un.org/en/udhrbook/.

Figure 3. Extent of application usage and data generation



Source: DOMO, Data never sleeps 6.0.

The General Data Protection Regulation issued by the European Union defines personal data as: "personal data' means 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".[23]

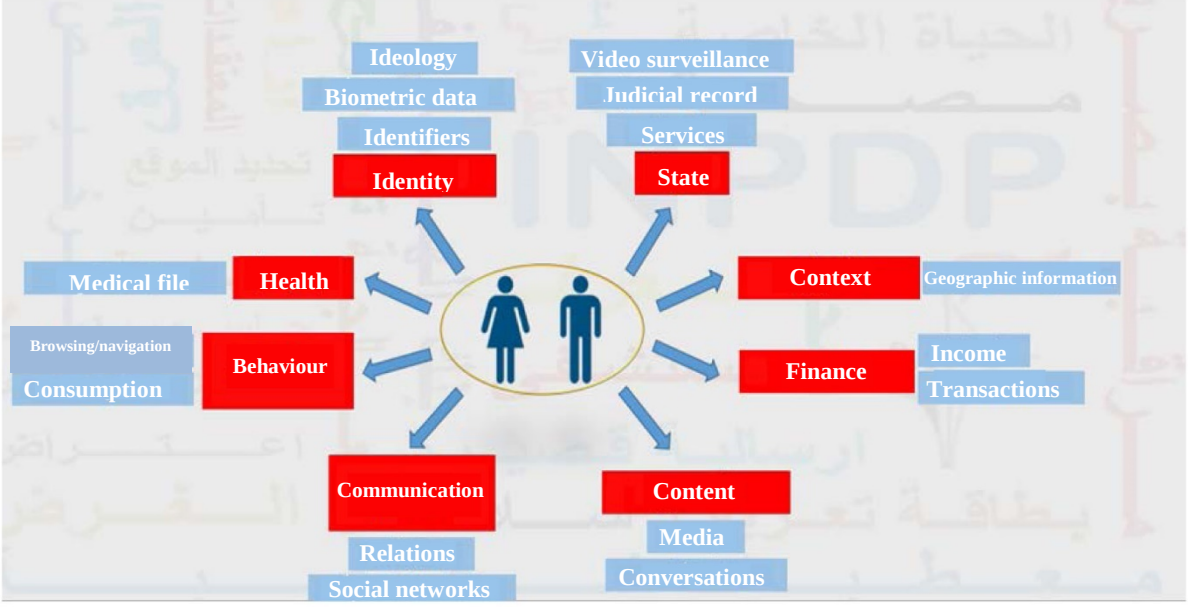
Personal data can therefore be defined as information that allows, directly or indirectly, to identification of a natural person or renders them identifiable.

Government agencies collect large amounts of data pertaining to citizens, and if published, such data can put their owners at risk. In fact, Government agencies collect, use and sometimes exchange such personal data, and are therefore responsible for protecting them from loss, theft and use.

Laws on personal data protection are aimed at controlling the use and transfer of private data by giving persons the right to control their personal data, imposing rules for the use of such data by institutions and Governments, and establishing regulatory bodies to monitor the application of laws. Legislation on personal data protection varies from one country to another, as many countries still have no laws in this area (only 130 countries have laws on personal data protection).

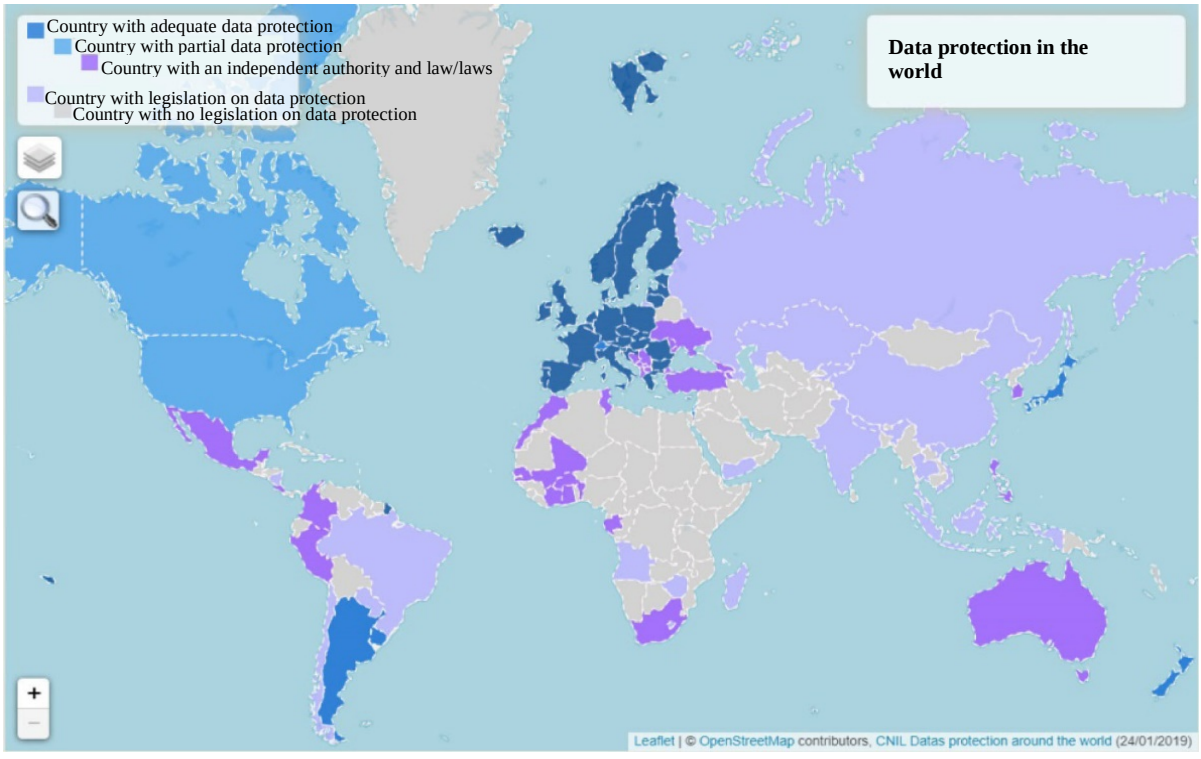
[23] https://gdpr-info.eu/.

Figure 4. Personal data



Source: National Authority for the Protection of Personal Data, Tunisia.

Figure 5. Global mapping of personal data protection (January 2019)



Source: Commission nationale de l'informatique et des libertés (CNIL), France.

Few Arab countries have passed legislation on the protection of personal data and private life, including Bahrain, Lebanon, Morocco, Qatar and Tunisia.

The OECD recommendations for the protection of private life[24] identified the principles of protecting personal data as follows:

- **Control of data collection**: setting limits for collecting personal data and ensuring data access in legal and impartial ways;
- **Quality of data**: personal data should be relevant to the purpose of use, true, complete and updated;
- **Purpose**: data should be used only for the purpose for which they were collected and not for other purposes;
- **Restriction of use**: data should not be used for other purposes without the consent of those concerned or the consent of a legal body;
- **Approval**: data are to be disclosed only with the consent of the persons concerned;
- **Storage**: collected data should be securely stored, away from any attacks;
- **Transparency**: it should be upheld in all matters relating to the development, uses and policies of personal data, with the provision of information on collected data, their purpose of use and persons handling them;
- **Participation**: data owners have the right to access, view, request access to, delete, correct, complete and modify their data;
- **Accountability**: mechanisms should be provided for data owners to track who collects their data without respecting these recommendations.

Personal data are one of the most important exceptions in access to information, as laws on the right of access exclude personal information and require withholding it when disclosing documents or statements containing such data. Since exceptions in the area of access to information are not absolute and are subject to the balance of harm and public interest, personal data are themselves subject to that balance. Therefore, laws on access to information allow the disclosure of personal data in the event that public interest prevails over the harm entailed by access to information. Otherwise, personal data cannot be disclosed and must be concealed.

Balancing the right to access information with the right to protect personal data is a difficult bet, as experts in personal data protection seek the complete closure of such data access under relevant laws. Nevertheless, experts in the field of access to information emphasize the need to prioritize laws on access to information and enable the balance of harm and public interest so as to decide whether to disclose personal data or not. In this context, the European General Data Protection Regulation, one of

[24] OECD recommendations for the protection of private life, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

the most stringent legislation on personal data protection, has made it possible to disclose personal data in order to reconcile public access to official documents with the right to the protection of personal data, as discussed in Article 86 of the Regulation.

Box 4. Article 86 of the European General Data Protection Regulation

"Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation".

Source: The European General Data Protection Regulation.

Legislation on private data protection is the second most important law in the area of open government, particularly in terms of transparency and access to information. The existence of these laws in Arab countries is timid compared to their large prevalence in other regions of the world. The promulgation of these laws remains a legislative priority in Arab countries, as many of them are currently drafting a law on the protection of personal data.

2. *Cybercrime laws*

Cybercrime legislation is one that limits access to information. It aims to protect data from attacks, piracy and unauthorised access, and thus to close access to information, particularly in unauthorised ways. It also limits the risk of attacks on open data, data falsification, disclosure of personal and confidential data, attacks on intellectual property, dissemination of prohibited information (e.g. racist content) and obstruction of the use of information systems. Therefore, cybercrime legislation helps to establish open government and aims to:[25]

- Develop clear standards of conduct for the use of computers;
- Deter criminals and protect citizens;
- Enable law enforcement authorities to conduct investigations, while protecting individual privacy;
- Ensure fair and equitable proceedings for criminal justice;
- Comply with minimum protection standards in areas such as handling and safeguarding data;
- Enable inter-State cooperation in criminal matters involving cybercrime and in electronic evidence.

[25] According to the United Nations Office on Drugs and Crime.

Cybercrime legislation protects open data and counters data falsification, impersonation, disclosure of confidential or personal information and other infringements of published and unpublished data and information. While the role of such legislation is essential in reducing and deterring such infringements, a number of them contain provisions that may curtail free access to information, or may contradict the provisions of laws on access to information. A number of them also deliberately or unintentionally reduce access to information and expand the scope of exceptions by prioritizing their provisions over other, more open and transparent provisions of laws.

3. *Intellectual property laws*

Intellectual property laws include:[26]

- **Industrial property**: it includes industrial designs and models, patents, trademarks and geographic information;

- **Literary and artistic property**: it consists of **copyright**, which includes literary and artistic works such as novels, poems, plays, musical works, oil paintings, photographs, sculptures, urban designs and information programmes; **related rights**, which include the rights of performers, producers of phonograms and broadcasting organisations to authorise or prohibit the use of their performances, recordings, and radio and television programmes, respectively.

Copyright represents the set of literary and material rights enjoyed by right holders in exchange for the use of their literary, artistic and scientific works. These are exclusive rights enjoyed by owners of innovative works in exchange for the use or authorized use of their works by third parties. No one has the right to transmit, publish or reproduce works in any form or method that violates their authors' physical and moral rights.

Intellectual property is an exception to access to information, as laws on the right to access information exclude information protected by intellectual property and require withholding it when disclosing documents or statements containing such data. Since exceptions in the area of access to information are not absolute and are subject to the balance of harm and public interest, information protected by intellectual property is itself subject to that balance. Therefore, laws on access to information allow the disclosure of information protected by intellectual property in the event that public interest prevails over the harm entailed by access to information.

Intellectual property laws determine the duration of copyright protection, which usually lasts for the authors' lifetime and for 50 years or more following their death. Intellectual property expires at the end of copyright protection, and the disclosure of such information becomes permissible. Since intellectual property is usually an exception covered by laws on access to information, information protected by intellectual property laws can only be accessed upon the expiry of copyright protection or if the public interest prevails.

[26] World Intellectual Property Organization (WIPO), What is intellectual property? https://www.wipo.int/edocs/pubdocs/en/intproperty/450/wipo_pub_450.pdf.

Open data licenses are considered as a type of intellectual property license, explaining the rights held by authors and those that authors waive to others in reusing, republishing, adding and modifying published data.

4. *Laws on confidentiality of information*

In light of the threats that the world is now facing and that involve the use of information and communication networks, particularly terrorist acts, many States have enacted laws on confidentiality of information, through which they have sought to protect access to sensitive and strategic data. Data related to public security and national defence are among the most important exceptions in the laws on the right to access information, as indicated in indicator 29 of RTI Rating: "The exceptions to the right of access are consistent with international standards. Permissible exceptions are: national security; international relations...". Most confidentiality laws are intended for certain groups, such as public security and defence personnel or State officials. They also pertain to the disclosing party and user of confidential information, similar to the press.

The legal provisions on confidentiality present four common elements:

- Protecting special categories of information (e.g. public security);
- Regulating private persons (e.g. private bodies);
- Preventing types of information-related activities (e.g. query);
- Exceptions where a person does not violate a confidentiality provision.

The first bet of these laws, particularly for States that adopt open government principles, remains to balance the right to access information and to uphold transparency with the right to protect access to sensitive and strategic data. Laws on confidentiality of information contradict those related to the right to access information, and their provisions are usually given more priority than the latter.

For example, the United Kingdom Official Secrets Act 1989 includes:[27]

- Quality of information:
    - Security and intelligence;
    - Defence;
    - International relations;
    - Crimes and investigation;
    - Information resulting from unauthorised disclosures or entrusted in confidence;
    - Information entrusted in confidence to other States or international organizations;
- Authorised disclosures;
- Safeguarding of information;
- Limitations on prosecution;
- Penalties;
- Arrest, search and trial.

[27] The United Kingdom, Official Secrets Act 1989.

The political and security conditions in the Arab region constitute an environment in which it is difficult to convince decision makers of the need to pass laws on the right to access information, given national and social security concerns among others. These laws conflict with pre-enacted laws, such as the Information Confidentiality Act. Therefore, finding some kind of balance between the law on the right to access information and laws that might overlap with it, such as the Information Confidentiality Act, has become an important and urgent matter, particularly in the context of the Arab region.

In this context, 22 non-governmental organizations developed a set of principles, in collaboration with more than 500 industry experts and with the support of the Open Society Foundations, at a meeting held in Tshwane, South Africa. These principles aim to strike a balance between the law on the right to access information and the Confidentiality of Information Act (box 5). A committee from the Parliamentary Assembly of the Council of Europe supported those principles and encouraged member States to align them with their relevant laws.[28]

Box 5. Tshwane Principles on National Security and the Right to Information

These principles (about 40 principles) are intended to support persons working in this field in enacting, reviewing or implementing draft laws to distinguish between cases where information should not be disclosed on the grounds of national security and those in which it should be disclosed. Principles are divided into groups, namely general principles; principles on information that may be withheld or disclosed; principles relating to the judicial aspect; the processing of information requests; institutions that oversee the security sector; and others.

The **first principle** states that everyone has the right to access and use information held by public institutions. No institution has the right to withhold such data, unless it is a governmental institution directly concerned with the protection of national security, as only this institution is entitled to withhold information on the grounds of national security protection. This does not include private institutions operating in the security sector, as only governmental institutions are responsible for protecting national security. The **fourth principle** stipulates that right to information should be broadly applied and the scope of exceptions narrowed, and that the public institution bears the burden of clearly and specifically demonstrating the reasons behind information restrictions. The **sixth principle** includes the right of oversight bodies, courts and judicial authorities to access information, regardless of its classification level, to properly discharge their responsibilities, while the **thirty-fifth principle** states that these institutions are responsible for applying all criteria that ensure the protection and confidentiality of information in their possession.

Source: The Global Principles on National Security and the Right to Information (Tshwane Principles), Open Society Foundation, Open Society Justice Initiative. Available at https://www.justiceinitiative.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles.

B. Laws supporting access to information

Some pieces of legislation encourage access to information by protecting users and giving them the right to seek access to and disseminate information. The right to information laws are considered as

[28] European Endorsement for Tshwane Principles on National Security and Right to Information, https://www.justiceinitiative.org/newsroom/european-endorsement-tshwane-principles-national-security-and-right-information (accessed on 6 April 2020).

an extension of these laws, as they are one of the mechanisms of action in areas they regulate, such as laws on the freedom of expression and freedom of the press.

Several pieces of legislation aim to regulate access to categories of information that are protected from dissemination, such as archived or statistical information. Such legislation regulates time limits for the public dissemination of protected data, such as personal data or data protected by intellectual property. This legislation plays an important role in opening data that are excluded from access to information laws, such as security and personal data, and data protected by intellectual property laws, upon the expiry of time limits stipulated by the legislation.

This legislation is generally considered to be appropriate and conducive for access to information. Some of those laws are presented below.

1. *Laws on freedom of opinion, expression and press*

The practice of media work is based on the following principles:

- Freedom of expression and fundamental freedoms of citizens;
- The right of citizens to access information on public affairs;
- Freedom and right of the media to search, access and disseminate information;
- Respect for the privacy and rights of individuals;
- Media professionals shall not be subject to prior censorship and shall be held liable for the published content;
- The right to ask media professionals to disclose their sources of information shall only be granted through the judiciary.

Media laws address the right to freedom of expression and the right to access and use data and information for media purposes. Media laws generally stipulate that all media outlets shall be independent and freely perform their mission in a transparent manner. They also provide for the right to access information.

Media outlets are the ones that advocate the most for the right to access information and for narrowing the scope of exceptions given the media content they derive from this right. This also applies to investigative and data journalism, which mainly relies on access to official data and documents.

Access to information laws are considered as an extension of press and media laws that rely on them to provide access to information. The press and media sector is one of the most prominent users of access to information laws and is a major supporter of the enactment of these laws, which provide journalists and media professionals with access to information mechanisms and a framework for requesting information.

2. *Archive laws*

The archive is the collection of documents that every natural or moral person, every public facility, public or private body has created or obtained during the course of their activity, regardless of the date, form and material support of these documents. Documents are stored and the archived assets are collected in the public interest to meet the needs of handling data, conducting scientific research, establishing the rights of persons and protecting national heritage.[29]

Legislation on archives regulates access to stored or archived information, and archival institutions are responsible for regulating and safeguarding official documents and information for later access by the public. They also work to protect documents in their possession from public access. These documents contain personal data, documents protected by intellectual property and security data. Archival institutions make documents in their possession available for public access upon the expiry of time limits stipulated by archive laws, and depending on the type of information and documents.

Archive laws contain provisions regulating access to archived documents as they set time limits for making documents available according to the type of information they contain. These laws help to access information, as they allow access to personal or security information, civil status or medical files upon the expiry of specific time lines depending on the type of document.

Box 6. Some provisions of the Tunisian law relating to archives and regulating access to archived documents

Article 15: Public archives can only be accessed after one year from the date of their establishment, except in cases provided for in articles 16 and 17 of the present law.

Article 16: The time line stipulated in article 15 above shall be raised to:

1. 60 years:

(a) From the date of establishment, for documents containing information affecting private life or relating to national safety;

(b) From the date of census or investigation, for documents collected in the framework of statistical investigations conducted by persons, institutions and bodies mentioned in article 3 of the present law, and containing information on the personal and family life of individuals and, generally, on their acts and behaviours.

(c) From the date of the decision or closing of the file, for documents relating to cases brought before judicial authorities.

2. 100 years:

(a) For documents of notaries and enforcement agents, civil status documents and registration files;

[29] Tunisian law No. 95 of 1988 dated 2 August 1988 relating to archives.

(b) From the date of birth of the persons concerned, for documents containing individual medical information and for the files of personnel.

Article 17: The National Archives may allow access to public archives before the expiry of time limits set out in articles 15 and 16 of the present law, for the purpose of scientific research, and after consulting the administration that created these documents, without any prejudice to personal life confidentiality or to national safety.

Article18: Notwithstanding the provisions of article 15 of the present law, public archives can be accessed prior to the expiry of 30 years, for documents designated by virtue of a decree.

Article 19: The conditions and arrangements for access to public archives shall be set by virtue of a decree.

Source: Tunisian law No. 95 of 1988 dated 2 August 1988 relating to archives.

3. *Statistics laws*

National statistical systems play a key role in the provision and opening of data. Most have developed open data portals that provide open statistical data for use and reuse by the public. States are seeking to develop their legislation on statistics to open further data while maintaining personal data confidentiality. The statistics legislation is aligned with open government principles, such as transparency, participation and accountability.

In 1994, the United Nations Statistical Committee adopted 10 principles for official statistics, which were voted upon at the United Nations plenary meeting on 29 January 2014. States rely on these principles in enacting legal texts for their statistical systems, and national statistical agencies are keen to comply with these principles. It should be noted that these principles are mostly aimed at achieving transparency, disseminating information and gaining the confidence of citizens by preserving their personal data.

Box 7. Fundamental principles of official statistics according to the United Nations Statistical Committee

1. Official statistics that meet the test of practical utility are to be compiled and made available on an impartial basis by official statistical agencies to honour citizens' entitlement to public information.
2. To retain trust in official statistics, the statistical agencies need to decide according to strictly professional considerations, including scientific principles and professional ethics, on the methods and procedures for the collection, processing, storage and presentation of statistical data.
3. To facilitate a correct interpretation of the data, the statistical agencies are to present information according to scientific standards on the sources, methods and procedures of the statistics.
4. The statistical agencies are entitled to comment on erroneous interpretation and misuse of statistics.
5. Data for statistical purposes may be drawn from all types of sources, be they statistical surveys or administrative records. Statistical agencies are to choose the source with regard to quality, timeliness, costs and the burden on respondents.
6. Individual data collected by statistical agencies for statistical compilation, whether they refer to natural or legal persons, are to be strictly confidential and used exclusively for statistical purposes.

7. The laws, regulations and measures under which the statistical systems operate are to be made public.
8. Coordination among statistical agencies within countries is essential to achieve consistency and efficiency in the statistical system.
9. The use by statistical agencies in each country of international concepts, classifications and methods promotes the consistency and efficiency of statistical systems at all official levels.
10. Bilateral and multilateral cooperation in statistics contributes to the improvement of systems of official statistics in all countries.

Source: United Nations Statistical Committee.

4. *Data classification*

States should develop a national system for government data classification, which allows:

- Developing a framework for the use and reuse of data;
- Regulating and protecting their information inventory;
- Creating a framework for government data governance;
- Achieving coherence between the system and laws, legislation and data handling regulations.

Government data classification systems aim to determine levels of classification by scope of disclosure, identify the necessary provisions for handling confidential data, and establish a framework for the governance of data classification.

Once the data classification model is certified, it will be easy to identify data that can be opened and to carry out an inventory of open data. The data classification model must include a category for "data completely open to the public". The data included in this category are directly and openly published.

Data classification is not necessarily determined by virtue of a law, but by Government order or instructions. It can also be included in one of the relevant laws, such as the Information Safety Act or open data legislation.

The data classification model must be in line with the Access to Information Act, and in no case can a request for access to information be denied on the grounds that it is confidentially classified, as classification systems must not conflict with rights of access to information.

Table 6. Data classification model

Restricted	Confidential	Internal	Public (open)
Highly sensitive data that can affect corporate security	Sensitive data that can affect operational integrity	Internal data not meant for public disclosure	Data that may be freely disclosed to the public

Source: Forsythe Solutions Group, 7 Steps to Effective Data Classification.

IV. The Legislative Framework for Civic Engagement

Civic engagement can take different forms, such as public consultations, forums, hearings, petitions, etc. Engaging citizens in various stages of policymaking and decision-making aims to listen to their concerns and involve them in public life to bring them closer to the administration and strengthen mutual trust between them and the Government.

The legislative framework for civic engagement usually consists of a set of texts governing various forms of public participation, such as public consultations and petitions.

A. Public consultations

Public consultations are one of the most important forms of civic engagement, as decision-makers seek to consult citizens on public policies, draft laws, major projects, etc., with the aim of strengthening trust with citizens. Legislation on public consultations aims to regulate the field of consultations, such as identifying sectors and areas involved in consultations and specifying how to conduct consultations, the duration of consultations, how to take note of consultation outcomes and the need to disseminate them.

Public consultations are usually regulated through Government orders or instructions. However, a number of States, such as Portugal and the United States of America, have relied on laws to regulate this field.[30]

Provisions relating to the organization of public consultations cover the following areas:

- Implementing provisions related to the organization of public consultations (relevant interests and topics);
- Preparing for the organization of public consultations (coordinator, subject, participants, format, course of action, etc.);
- Launching public consultations;
- Monitoring and evaluating public consultations;
- Undertaking actions for the proper organization of public consultations (finance, training...);
- Possibly holding hearings.

B. Petitions

Petitions are written demands containing claims, proposals or recommendations addressed by a person or group of persons to their governments or parliaments with a view to taking action accordingly. These broad demands expressed by the public can be supported, and the number of supporters is essential in determining the type and scope of actions that public authorities should undertake.

[30] Background Document on Public Consultation, OECD, P4, https://www.oecd.org/mena/governance/36785341.pdf.

Petitions are filed with higher authorities with a view to taking the necessary decisions accordingly. They can also be referred, depending on the number of signatories. The regulatory texts of petitions take the form of Government orders or laws. Laws on the right to submit petitions to public authorities include, among others, the following provisions:

- Require that the petition aims to achieve the public interest;
- Identify areas of exception, such as petitions related to security, defence and justice, and those pertaining to political, trade unionist or discriminatory affairs;
- Collect a minimum number of supporters' signatures and submit the petition along with a validation of signatures;
- Refer the petition to the intended recipient once the minimum number of supporters' signatures is collected;
- Appoint a committee at the office of the Prime Minister or Speaker of Parliament to sort, monitor and express an opinion on petitions;
- Inform petition authors of the decisions taken.

V. Other Legislation on Accountability

Accountability is one of the principles of open government and ensures that governments take responsibility for their decisions and actions. Laws on the right to access information, integrity, anti-corruption, protection of corruption whistle-blowers, and declaration of gains and assets are among the most important legislation upholding accountability.

A. Laws on integrity, anti-corruption and protection of corruption whistle-blowers

Laws on anti-corruption and protection of corruption whistle-blowers aim to control the forms and procedures for reporting corruption and for protecting whistle-blowers, therefore enshrining the principles of transparency, integrity, accountability, good governance and the prevention and fight of corruption in the public and private sectors. These laws also establish independent oversight bodies tasked with developing policies and systems to prevent, combat and detect corruption, and monitoring the implementation of such policies.

The provisions of both Anti-Corruption and Whistle-blower Protection Acts include:

- Identifying the body responsible for receiving reported corruption cases;
- Arranging the forms and procedures for reporting corruption cases;
- Setting the terms and mechanisms for protecting whistle-blowers;
- Protecting whistle-blowers;
- Assisting whistle-blowers;
- Granting a financial reward to whistle-blowers;
- Preserving the anonymity of whistle-blowers;
- Imposing penalties on those who deliberately disclose the whistle-blower's identity.

B. Laws on the declaration of gains and assets

Laws on the declaration of gains and assets are one of the most important laws for achieving open government, and one of the most important preconditions for entering into an open government partnership. Gains are declared before a governmental or independent authority that is determined by law.

The designated and elected persons who are entrusted with powers of the public authority, State officials or a public institution and anyone who has the status of a public officer are subject to the provisions of these laws. In many States, declarations of senior State officials must be publicly disclosed and published under the provisions of the law.

VI. Conclusions and Recommendations

A. Conclusions

The concept of open government is based on good governance principles, the most important of which is the transparency of government action, the achievement of citizens' right to access government information and their engagement in policy making and decision-making, and the development of mechanisms for holding governments accountable. Open government is one of the pillars for the implementation of the SDGs, particularly SDG 16, which aims to spread “peace, stability, human rights and effective governance, based on the rule of law”. Open government contributes to accelerating efforts to end poverty (SDG 1), by making institutions more transparent and effective, thereby giving citizens a role in controlling public expenditure. It fosters innovation (SDG 9), as open data help individuals, the private sector and non-governmental organizations to develop innovative community applications. Furthermore, reliance on open data and participatory planning contributes to better planning, distribution and monitoring (SDGs 6, 7 and 8).

Open government data policies uphold transparency, accountability and value-added creation, through universal access to government data. Government institutions, which have large amounts of data and information, can become more transparent and accountable by opening their data to the public. They can also provide better services for citizens by encouraging the free use, reuse and distribution of such data, thereby helping their Governments to establish start-ups and create new employment opportunities.

Open data differ from open government, although both terms are interlinked. Through digital publishing and reuse of government data, open data can support transparency, cooperation and participation, which are the basic principles of open government.

Legislation on the promotion of open government and open data is mainly legislation on the principles of open government, i.e. participation, transparency and accountability, and the opening and dissemination of government data for public reuse. The study tackled laws that have a significant impact on aspects of open government principles, particularly transparency and the right to access open information and data.

Laws on the right to access information are an essential part of open government legislation. They help to uphold transparency in government action by requiring public institutions to disclose government information and to automatically publish a number of documents and data, therefore allowing the fight against various forms of corruption such as bribery and cronyism within the public sector. Access to information laws can be seen as the cornerstone of a governance system based on transparency and accountability, and as a pillar of the open government system.

The legislative framework for open data contains legal aspects, including the right of citizens to access, reuse and distribute government data. It also includes regulatory aspects related to the management of the open government data programme, the development of open data portals, data description, data quality, free of charge government data, governance of the open data programme, etc.

Studies and work completed with regard to the law on the right to access information have revealed that the provisions of many other laws may interfere with this right. Therefore, these laws must be reviewed to ensure that access to information laws are prioritized over other related laws.

The present report addressed a number of legislation related to open government and the right to access open information and data. These laws fall into two categories: laws restricting the right of access and, therefore, restricting and narrowing access to information; and laws upholding the right of access and, therefore, encouraging and providing mechanisms to access information in specific sectors.

Laws on personal data protection are aimed at controlling the use and transfer of private data by giving persons the right to control their personal data, imposing rules for the use of such data by institutions and Governments, and establishing regulatory bodies to monitor the application of laws. They are among laws that limit the right of access, yet they are essential to strengthen open government, given their role in protecting persons' private lives that become threatened if their data are published.

Intellectual property is one of the exceptions to information access, as access laws exclude information protected by intellectual property and require withholding it when disclosing documents or statements containing such data. Access to information laws also require disclosing intellectual property data when the relevant reasons cease to exist.

The first bet of these laws on confidentiality of information, for States adopting open government principles, remains to balance the right to access information and to uphold transparency with the right to protect access to sensitive and strategic data. Laws on confidentiality of information contradict those related to the right to access information, and their provisions are usually given precedence over the latter.

Cybercrime legislation is also one that limits access to information. It aims to protect data from attacks, piracy and unauthorised access, and thus to close access to information, particularly in unauthorised ways.

Media laws address the right to freedom of expression and the right to access and use data and information for media purposes. Media laws generally stipulate that all media outlets shall be independent and freely perform their mission in a transparent manner. They also provide for the right to access information. Media outlets are the ones that advocate the most for the right to access information and for narrowing the scope of exceptions given the media content they derive from this right and the support they get for investigative and data journalism, which primarily relies on access to public data and documents.

Archive laws contain provisions regulating access to archived documents as they set time limits for making such documents available according to the type of information they contain. These laws help to access information, as they allow access to personal or security information, civil status or medical files upon the expiry of specific time lines depending on the type of document.

National statistical systems play a key role in the provision and opening of data. Most have developed open data portals that provide open statistical data for use and reuse by the public. States are seeking to develop their legislation on statistics to open further data while safeguarding personal data.

Countries that adopt open government principles need to strengthen a national system for the classification of government data. The data classification model must be in line with the provisions of the Access to Information Act. In no case can a request for access to information be denied on the grounds that it is confidentially classified, as classification systems must not conflict with rights of access to information.

B. Recommendations

1. Access to information laws are the cornerstone of a governance system based on transparency and accountability, and a pillar of the open government system. Therefore, it is necessary to pass a law granting the right to access information, as a starting point towards implementing open government.

2. Laws on the right to access information vary from one country to another, in terms of openness, disclosure stakeholders and safeguards for information access. This prompted global institutions to develop methodologies for evaluating and classifying laws. Since the degree of openness in these laws is very much related to the political, cultural and security realities of States, many open government methodologies do not attach great importance to the value of provisions contained in access to information laws, but rather focus on the mandatory enactment of laws in this area.

3. Enacting a law on the right to access information requires a number of basic principles that must be covered by the provisions of the law, including respecting the principle of maximum disclosure and limiting exceptions, not exempting any public institutions from the duty to disclose, facilitating ways of requesting and obtaining information, ensuring access to information, and granting the right to appeal the decision of refusal and the right to litigation, etc.

4. Access to information laws vary in terms of their compatibility with these principles. Globally, most laws are not fully compatible with these principles; therefore, there is a need to review them or re-enact new laws. Entrenching the culture of the right to access government information and developing access practices remain one of the most important objectives of these laws.

5. Adhering to an open government partnership requires compliance with a number of criteria, the most important of which is the adoption of laws and legislation including a law that regulates access to information and incorporates this right in the Constitution, and a law on the asset declaration of public officials.

6. The utmost effectiveness of laws on access to information requires effective implementation of these laws, which necessitates the will and commitment of Governments to ensure access to information. The law is not the only means to eradicate corruption; it must be accompanied by other measures such as simplifying and digitizing administrative methods, and educating and strengthening the integrity of public servants so that corruption outlets are eliminated and blocked.

7. In drafting the Access to Information Act, it is useful to be guided by evaluation indicators, such as RTI Rating indicators, to determine the law provisions and maximize compliance with these indicators to safeguard the law value.

8. Legal aspects of open data are usually included in the Access to Information Act. This law should include provisions concerning the automatic dissemination of information, the right to reuse government data and the need to publish a licence for reuse. In this case, the regulatory aspects of open data are included in regulatory orders or instructions published in the Official Gazette.

9. It is possible to enact a stand-alone law on open government data, provided that it contains provisions relating to the reuse of government data, the need to publish a reuse license, and other regulatory provisions, such as programme governance and free open data.

10. Since access to open data is primarily aimed at reusing data to create added value, legal provisions must be adopted allowing the unrestricted reuse of open government data, except in cases of intellectual property considerations. There must also be legal provisions stipulating the need to issue a reuse license for each published data set in order to safeguard the rights of parties publishing or reusing such data.

11. Legislation on private data protection is the second most important law in the area of open government, particularly in terms of transparency and access to information. These laws, despite their large prevalence in the world, exist only timidly in Arab countries. The promulgation of these laws remains a legislative priority in Arab countries, as many of them are currently drafting a law on the protection of personal data.

12. The balance between the right to access information and the right to protect personal data is a difficult bet. Experts in the field of personal data protection seek to block access to such data by virtue of personal data protection laws. Nevertheless, experts in the field of access to information emphasize the need to prioritize laws on access to information and enable the balance of harm and public interest so as to decide whether to disclose personal data or not. Today's trend is to disclose personal data with the only aim of reconciling the right to access government documents with the right to protect personal data, if the public interest so requires.

13. Global standards provide for prioritizing laws on the right to access information over other relevant laws, such as laws on personal data protection, intellectual property, archives or statistics, and for including these areas in the exceptions to the access to information law, and therefore implementing the provisions of these laws in relation to access to protected information. The balance of harm and public interest should be weighed to decide whether to disclose such data or not, if the public interest so requires.

Bibliography

الإسكوا (2018). تعزيز الحكومة المفتوحة في المنطقة العربية. E/ESCWA/TDD/2018/TP.1. متوفر عبر الرابط: https://www.unescwa.org/sites/www.unescwa.org/files/publications/files/fostering-open-government-arab-region-arabic.pdf.

الإسكوا (2012). إرشادات الإسكوا للتشريعات السيبرانية. E/ESCWA/ICTD/2011/Technical Paper.5. متوفر عبر الرابط: https://www.unescwa.org/sites/www.unescwa.org/files/page_attachments/directives-full.pdf.

الجمهورية التونسية (2012). الهيئة الوطنية لحماية المعطيات الشخصية. مجموعة النصوص القانونية المنظمة لحماية المعطيات الشخصية. متوفر عبر الرابط: http://www.inpdp.nat.tn/Receuil_2019.pdf.

الجمهورية التونسية. هيئة النفاذ الى المعلومة. نصوص قانونية. متوفر عبر الرابط: http://www.inai.tn/textes-juridiques/.

دبي الذكية. بيانات دبي: اللوائح والأنظمة. متوفر عبر الرابط: https://www.smartdubai.ae/ar/data/regulations.

سعيد المدهون، البنك الدولي. الحق في الحصول على المعلومات في منطقة الشرق الأوسط وشمال أفريقيا: عرض عام لآخر التطورات والمستجدات في الأردن ولبنان والمغرب وتونس. متوفر عبر الرابط: http://documents.albankaldawli.org/curated/ar/202131467991020947/pdf/80668-WP-Almadhoun-ATI-in-MNA-Region-ARABIC-Box-393222B-PUBLIC.pdf.

سلطنة عُمان. عُمان الرقمية. سياسة البيانات الحكومية المفتوحة، متوفر عبر الرابط: https://opendata.moe.gov.om/images/library/file/Book334839.pdf.

المملكة الأردنية الهاشمية. وزارة الاتصالات وتكنولوجيا المعلومات. سياسة البيانات الحكومية المفتوحة. متوفر عبر الرابط: https://modee.gov.jo/uploads/Policies-and-Strategies-Directorate/Policies/Open-Government-Data-policy.pdf.

المملكة المغربية. اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي. التشريعات الخاصة بحماية المعطيات الشخصية. متوفر عبر الرابط: https://www.cndp.ma/ar/espace-juridique/textes-et-lois.html.

المنظمة العالمية للملكية الفكرية. ويبو ليكس. قوانين ومعاهدات الملكية الفكرية. متوفر عبر الرابط: https://wipolex.wipo.int/ar/main/legislation.

European Union (EU). Directive 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information.

EU, The European General Data Protection Regulation (EU) 2016/679. https://gdpr-info.eu.

Jérôme Denis, Samuel Goëta (2017). Les facettes de l'Open Data : émergence, fondements et travail en coulisses. Pierre-Michel Menger; Simon Paye. Big data et traçabilité numérique. Les sciences sociales face à la quantification massive des individus, pp. 121-138.

Lucie CLUZEL-METAYER et Elise MOURIESSE, « L'open data : une évolution juridique ? Propos introductifs », Revue générale du droit (www.revuegeneraledudroit.eu), Etudes et réflexions 2018, numéro 1.

M. A. TROJETTE (2013). « Ouverture des données. Les exceptions au principe de gratuité sont-elles toutes légitimes ? », Rapport au Premier ministre. https://www.etalab.gouv.fr/remiserapporttrojettesurlesexceptionsauprincipedegratuitedesdonneespubliques.

Organization of Economic Cooperation and Development (OECD) (2013). THE OECD Privacy Framework. OECD Publishing. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

_____ (2013). Regulatory Reform in the Middle East and North Africa: Implementing Regulatory Policy Principles to foster inclusive growth, OECD Publishing, https://www.oecd-ilibrary.org/governance/regulatory-reform-in-the-middle-east-and-north-africa_9789264204553-en.

_____ (2019). Institutions Guaranteeing Access to Information: OECD and MENA Region. OECD Publishing. Paris. https://doi.org/10.1787/e6d58b52-en.

_____ (2017). Open Government Data: Towards Empirical Analysis of Open Government Data Initiatives. OECD Publishing. Paris. https://www.oecd-ilibrary.org/docserver/5k46bj4f03s7-en.pdf?expires=1576833704&id=id&accname=guest&checksum=77B66437F8BFD87521A4D979D3F86558.

Access Info Europe & The Centre for Law and Democracy. The RTI Rating: analyses the quality of the world's access to information laws. https://www.rti-rating.org.

Toby Mendel, Centre for Law and Democracy (2013). Handbook on International Standards and Media Law in the Arab World. http://www.law-democracy.org/live/wp-content/uploads/2012/08/Handbook.IFJ-CLD-MENA-region.13.08.pdf.

Victoria L. Lemieux and Stephanie E. Trapnell (2016). Public access to information for development: a guide to effective implementation of right to information laws, World Bank Publications.

20-00127