DIGIntegrity

Digitally transforming the fight against corruption

CAF BANCO DE DESARROLLO DE AMÉRICA LATINA

Title: DIGIntegrity: Digitally Transforming the Fight Against Corruption Legal

Deposit: DC2022000457

SBN: 978-980-422-263-4

Publisher: CAF

Responsible Editors: Camilo Cetina and Carlos Santiso, Physical Infrastructure and Digital Transformation Management.
Physical Infrastructure and Digital Transformation Manager, Antonio Silveira

Prepared under the direction of Carlos Santiso, formerly responsible for the State's Digital Innovation Directorate, and Claudia Flores, Director (E) of Digital Transformation.

The coordination, editing and preparation of the chapters was the responsibility of Camilo Cetina, Main Lead of CAF's public integrity agenda. With the support of: Paula Cruz Manrique as research assistant and Maffert Lizcano, CAF intern.

Publication coordination: Nathalie Gerbasi, Training Director (E).

The ideas and approaches contained in this edition are the sole responsibility of the authors and do not represent the official position of CAF.

Graphic design: Gastón Cleiman.

Cover photo: 12 Best Social Media Stocks To Buy Now, Almario, 2021.
Other publication photos: pexels.com and unsplash.com

This and other publications on Digital Transformation in: scioteca.caf.com

ACKNOWLEDGMENTS

This report has been prepared under the guidance and supervision of Carlos Santiso, formerly responsible for the Directorate for State Digital Innovation, and Claudia Flores, director (E) of the Digital Transformation Directorate, attached to the Physical Infrastructure and Digital Transformation Management of CAF - Development Bank of Latin America. The coordination, consolidation and drafting of the report was the responsibility of Camilo Cetina, senior executive and leader of CAF's public integrity agenda.

This report is based on a set of studies carried out specifically for this project. CAF would like to thank the persons mentioned below for the insights, contributions and analyses, as well as for the comments and clarifications provided in the drafting of each chapter.

Chapter 1: prepared by Camilo Cetina, with the assistance of Paula Cruz Manrique.

Chapter 2: **Section 2.1**, prepared by Gustavo Fajardo and Jorge Gallego.
Section 2.2, prepared by Camilo Cetina, with inputs from Ana María Niño Ardila.
Section 2.3, prepared by Gustavo Fajardo, Jorge Gallego and Camilo Cetina.

Chapters 3, 4 and 6: prepared by Camilo Cetina, with the assistance of Paula Cruz Manrique. Section 3.2.3 is based on the work of Cetina, Garay Salamanca, Salcedo-Albarán and Vanegas (2021).

Chapter 5: prepared by Camilo Cetina, with inputs from Erick Rincón Cárdenas and assistance from Paula Cruz Manrique.

We also thank the following team of CAF specialists for their valuable review and comments to improve the document: Pablo Sanguinetti, formerly Vice President of Knowledge; Andrés Zamora and Martha Eloína Hernández, from the Strategic Communication Directorate; María Isabel Mejía, Nathalie Gerbasi and Enrique Zapata, from the Digital Transformation Directorate; Anabella Abadi, from the Impact Evaluation and Policy Learning Directorate; and Gustavo Fajardo, from the Socioeconomic Research Directorate. The publication was coordinated by Nathalie Gerbasi, with the support of Lorena López and Maffert Lizcano, from the Digital Transformation Directorate.

INDEX

INTRODUCTION

The well-known and unprecedented corruption scandals that occurred in Latin America during the last decade suggest that the region faces a phenomenon of institutional macro-cooptation (Garay, Salcedo-Albarán and Macías, 2018; Garay and Salcedo-Albarán, 2021). This means that there is coordination between private and public sector agents to control the provision of State goods and services as well as its institutions and norms. The fight against corruption and its criminal networks' impunity is a fundamental part of the development agenda which aims to end poverty, reduce extreme inequalities and, in the post-pandemic context, to facilitate economic reactivation.

According to various estimates, corruption —understood as the abuse of entrusted power for private benefit— could be costing between 2% and 5% of the world's Gross Domestic Product (GDP) (CAF, 2019; UN, 2018). This has adverse effects on the functioning of democracy and market economy. The World Economic Forum (WEF, 2019) estimates that corruption costs the developing world USD 1.26 trillion a year. According to data from the OECD (by its Spanish acronym) (2019d) that amount is equivalent to 7.5 times the annual size of its development aid. Transparency International (2021) has also documented corruption's potential effect on the deterioration of democracies and human rights violations.

Simultaneously, the world is witness to the digital acceleration of economies, governments and societies. Digitalization has positive effects on the economy: the United Nations estimates that the Information and Communications Technology (ICT) sector employs 2% of the world's population; represents a subscribed capital (in platforms alone) of more than USD 7 trillion; and, can contribute 15% of global GDP (UNCTAD, 2019). At the same time, coupled with economic globalization, the digital revolution also opens room for corruption networks to grow and increase their capacity for damage by operating in cyberspace without territoriality thus limiting governments jurisdictional capacities for their detection and sanction (Shelley, 1998).

In fact, Transparency International (2021) coined the concept of **"modern forms of corruption"** which links two types of phenomena: (i) those that are transnational in nature, and (ii) those that require the use of technology to illicitly acquire, move or dispose of assets obtained after the commission of crimes. Famous cases such as Lava Jato, Odebrecht, Panama Papers and FIFA-Gate are examples of modern forms of corruption. As the digitalizing of economies and telecommunications progresses it increases the potential for corruption networks to operate on a global scale, identify new means of cooperation, seek ways to exploit proceeds of corruption and accumulate profits obtained through transnational operations. This simultaneously grows their ability to reorganize and to hide among countless amounts of data within the technological platforms that transact money globally.

Surprisingly, literature linking the digital revolution to corruption control is still in its infancy (Haafst, 2017). Nevertheless, during the past decade, governments and other digital ecosystem actors have begun to **document experiences** on the potential and impact of digitalization in the promotion of transparency, in opening government data to public scrutiny, automatizing bureaucratic processes, restricting officials' discretion and limiting citizens' interaction with public officials to access essential services.

This report contributes to the state of the art by linking the concepts of digitalization and integrity and by proposing a public policy structure based on the adoption of digital innovations to prevent, detect and investigate corruption. The irruption of technology into the field of integrity has at least three major mechanisms of action:

1. By expanding access to information and opening data citizens have more information about their rights in their interaction with governments[1].

2. The advancement of digital government allows the simplification of administrative processes, and the streamlining of regulatory policy and open data infrastructures. Digitalizing procedures reduces bureaucratic discretion and opportunities for bribery.

3. The use of data analytics techniques as anti-corruption devices by integrity actors inside and outside of government enables a proactive and predictive approach to systemic corruption risk management (Cetina, 2020; Santiso, 2021).

Digitalization and its potential for public integrity is recognized in international arenas seeking to influence this agenda around the world. In 2018, the World Economic Forum launched the **Tech4integrity**, initiative, which serves as a global marketplace of technological innovations for integrity. In 2019, the **OECD** held the **Global Anti-Corruption and Integrity Forum**. The forum examined the potential of digital technologies like blockchain, artificial intelligence and open data to address a range of subjects spanning from bribery prevention to whistleblower protection. As a result, the OECD coined the term "Dig-Integrity". In 2020, the World Bank further promoted the expansion of digital technologies within governments seeking to adopt better integrity and anti-corruption policies through the **T4I** initiative. Finally, in 2021, the UN's General Assembly held a **Sesión Especial** Against Corruption which **explicitly endorsed the use of digital technologies** to facilitate access to information, promote accountability and prevent risks ranging from conflict of interest to money laundering.

[1] This is not a minor problem: for example, in 2019, petty bribery alone cost the Mexican economy USD 650 million, according to the statistics agency (Santiso, 2021).

Despite the remarkable awareness emerging around the world on the nexus between digital acceleration and public integrity policies, **there is still no comprehensive guide for governments to adopt anti-corruption mechanisms with a digital innovation approach. This report aims to fill that gap**, so public sector authorities and other integrity ecosystem actors can identify the best way to formulate and successfully implement a DIGIntegrity or T4I type anti-corruption agenda (Santiso, 2020) by combining six essential components, as detailed below:

- The concepts of proactive transparency and open data as enablers for any form of digital development to successfully operate in the integrity and anti-corruption ecosystem. Chapter 1 addresses the right to access public information and the datasets that make it up; as well as technical and institutional conditions for governments' incorporation of digital components into public integrity policies.

- Digital government and the State's digital transformation. Chapter 2 recognizes that digitalizing government public services precedes more sophisticated processes, such as investigating and sanctioning corruption. In particular, this chapter shows how higher levels of government digitalization correlate with lower risks of corruption. It also documents, quantitatively and qualitatively, the development of specific aspects in digital governance that affect public spending and citizen trust.

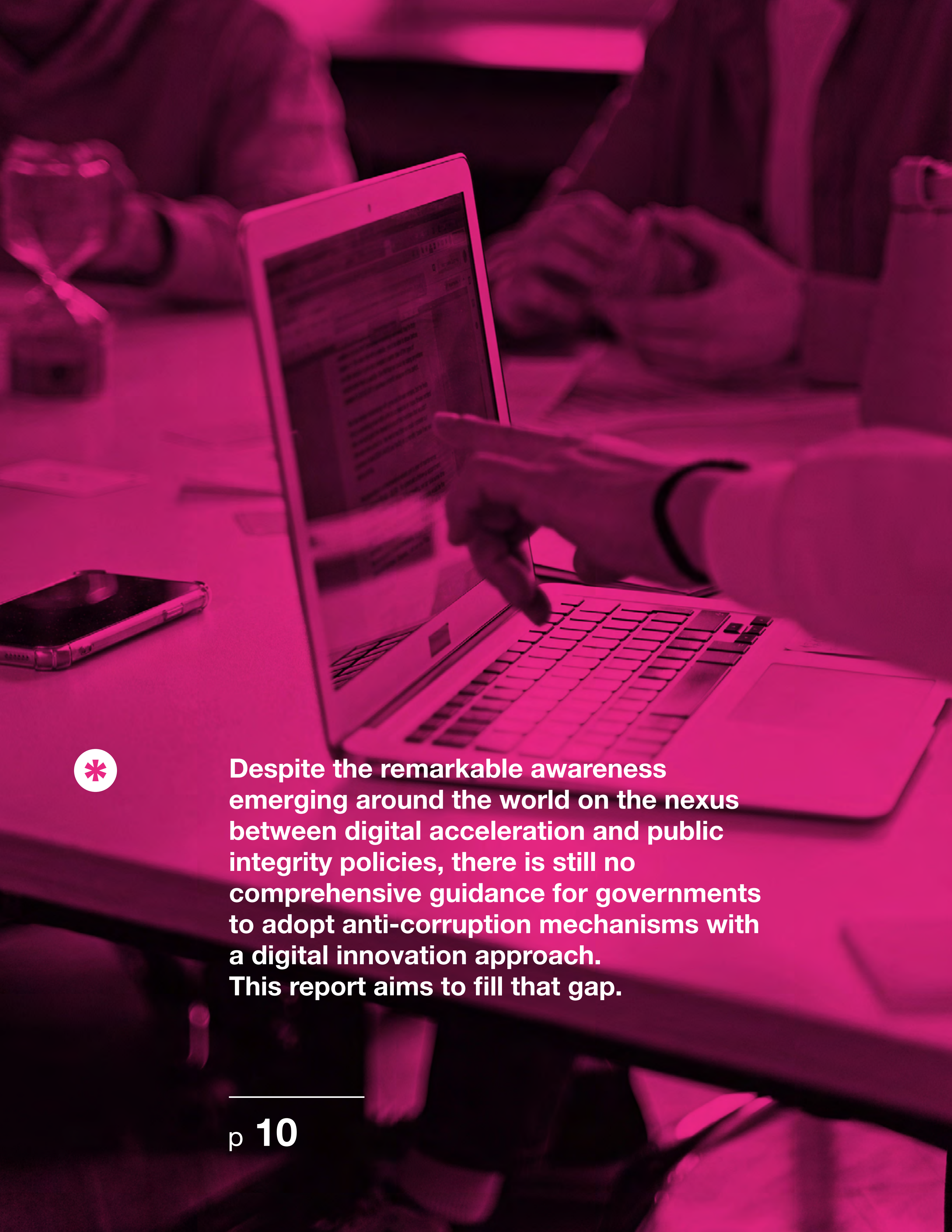
- Development of the main data reuse techniques to fight against corruption. Chapter 3 considers that articulating digital government, transparency and open data policies generates an ecosystem that reuses data and successfully applies data science and artificial intelligence to prevent and investigate corruption. The chapter also documents results from various actors within this ecosystem: private sector, civil society, control bodies and public procurement agencies.

- Uses of disruptive technologies such as blockchain for integrity. Despite the controversy surrounding this technological innovation, Chapter 4 documents blockchain uses that, as a proof of concept, show potential for reducing corruption risks in specific and particularly vulnerable processes such as public procurement, conditional cash deliveries, and coronavirus vaccine supplies. Again, there is an order preceding this technology: applying data science enables governments to develop digital infrastructures (Chapter 3), which makes it possible to invest in large computing power. The latter is a condition —almost an infrastructure— for blockchain's proper functioning.

- Technological risk management. Chapter 5 recognizes that the adoption of digital technologies helps to reduce corruption risks, but is not exempt from misuse. Just as there is technology for integrity, integrity in the use of technology must be ensured. This chapter discusses some aspects of technological risk management that governments should consider. These vulnerabilities are fueled by some of the legal and institutional loopholes that surround the adoption of digital technologies. Some examples explored here are the misuse of personal data, digital identity theft or the sophistication of criminal networks for money laundering through, for instance, the use of crypto-assets.

- Public policy recommendations to ensure optimal formulation and implementation of a technological innovation agenda in the service of public integrity. Compiled in Chapter 6, these recommendations demand on the one hand, the development of institutional adjustments to strengthen integrity in public policies; and on the other, the creation of necessary resources for digital innovation in public authorities belonging to the integrity ecosystem.

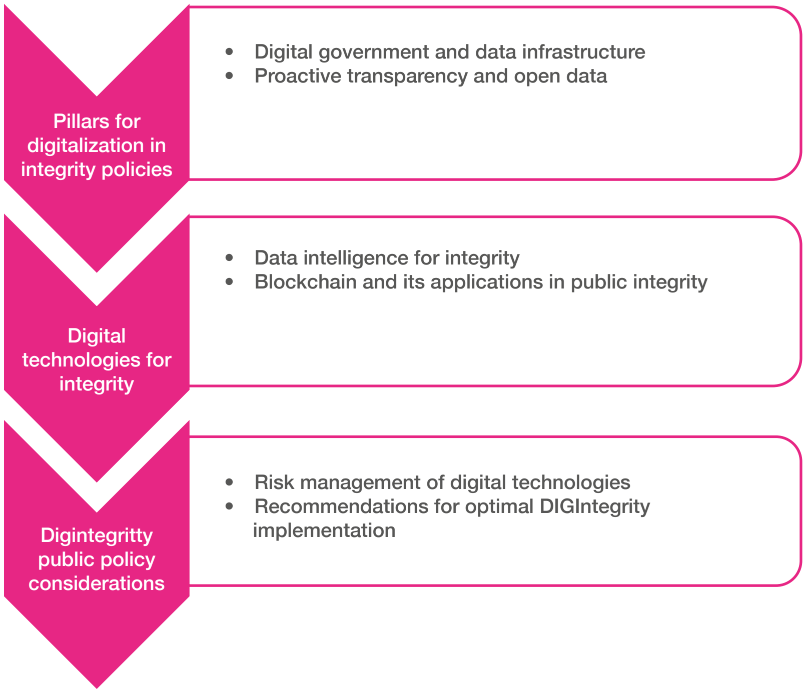
Figure 1 presents this report's structure. It is also a general outline to formulate a public integrity policy that leverages digital technologies, with a key assumption: digitalization in the fight against corruption does not begin nor end with the simple development of technological platforms to investigate or detect misconduct in public management.



Despite the remarkable awareness emerging around the world on the nexus between digital acceleration and public integrity policies, there is still no comprehensive guidance for governments to adopt anti-corruption mechanisms with a digital innovation approach. This report aims to fill that gap.

Figure 1

Report structure and proposed digitalization policy for integrity


Pillars for digitalization in integrity policies
- Digital government and data infrastructure
- Proactive transparency and open data
Digital technologies for integrity
- Data intelligence for integrity
- Blockchain and its applications in public integrity
Digintegritty public policy considerations
- Risk management of digital technologies
- Recommendations for optimal DIGIntegrity implementation

Source: Own elaboration.

This way, the successful incorporation of digitalization elements in the fight against corruption requires implementing several public policy initiatives, as follows:

- **Strengthen and guarantee access to public information through open data and functioning citizen digital services**. This is the only way for governments to develop data infrastructures, which are the raw material for technologies to function and generate results.

- Once governments have **data infrastructures** in place and implement **proactive transparency** standards, the window of opportunity opens to implement digital anti-corruption technologies through data reuse. This report illustrates the use of **data intelligence against corruption**, because its predictive capabilities help to prevent and expedite judicial investigations in this area.

- To adopt these technologies, governments must invest in **digital infrastructure with computing power**. Well-established computing and data infrastructures offer an opportunity for governments to explore blockchain as a way to protect governance processes from capture by improper interests.

- Complementary, this report considers that integrity policies based on digital technologies need a component that adopts transparency and integrity standards within digitalization itself. For this reason, we address some considerations about the **risk management** involved in the adoption of such technologies.

- Finally, adequate integrity policy management also requires modernizing **legal and institutional arrangements** in order to make the fight against corruption more preventive and restorative when prevention fails; and for the digital environment to facilitate innovation and modernization in this task.

Public integrity implies adopting a comprehensive approach that includes developing technological platforms and implementing conditions ranging from the consolidation of an open data agenda and quality datasets, to investment in computing and data infrastructure and risk insurance for new technologies. This report provides tools to implement digital anti-corruption agendas aligned with the needs, constraints and context of each country.

1. Qualifying conditions

“Data, data, data!” he cried impatiently. “I can’t make bricks without clay!”.

Sir Arthur Conan Doyle, The Mystery of Copper Beeches, in The Adventures of Sherlock Holmes

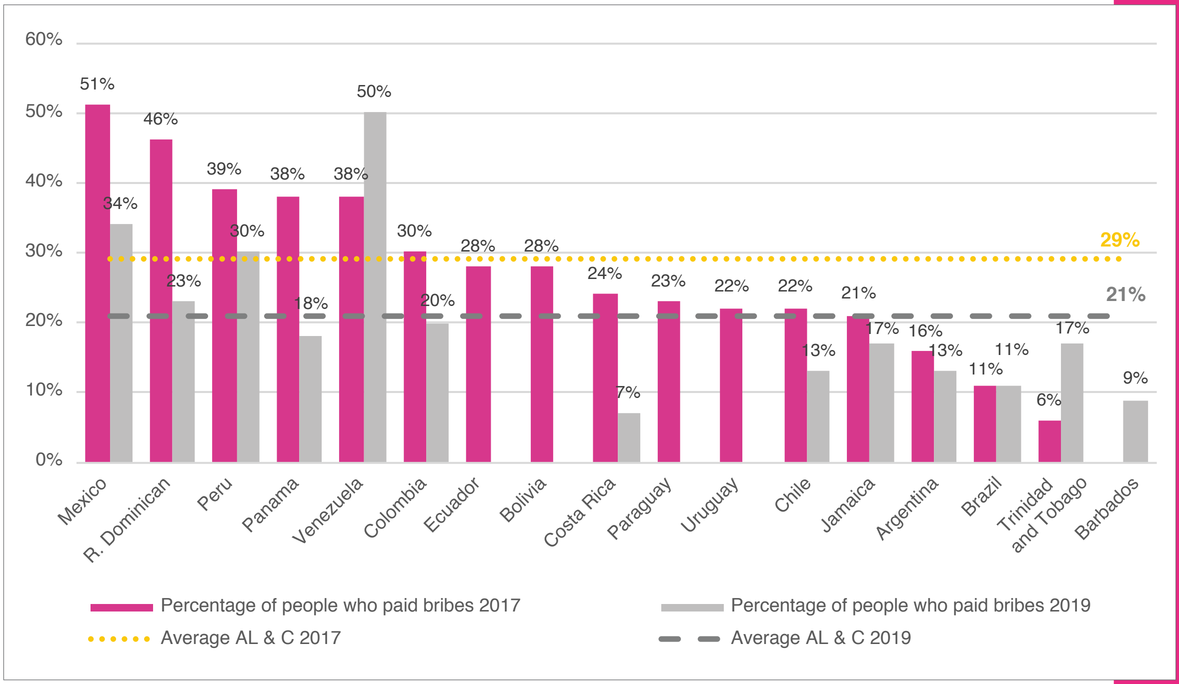
Qualifying conditions

Corruption involves the abuse of entrusted power for the purpose of misappropriating private benefits. This manifests itself in a variety of behaviors such as the illicit appropriation of public resources, the payment of bribes, conflicts of interest in government actions, and, on occasions, it is also linked to crimes like money laundering or smuggling. Corruption is particularly concerning to governments because the plundering of public assets impedes growth, contributes to inequality and hinders innovation (WEF, 2017).

Despite the persistence of corruption, Latin America has shown that it is possible to mitigate its risks. According to the 2017 Global Corruption Barometer, on average 29% of surveyed citizens in Latin America and the Caribbean reported having paid a bribe to access basic public services[2] such as education, health and identity documents (Transparency International, 2017). In 2019's barometer measurement the regional average decreased to 21 % (Transparency International, 2019). In 2017 in Mexico, **one in two respondents** (51 %) reported having paid a bribe to access basic public services (Transparency International, 2017) and by 2019, that number had decreased to 34 %.

[2] The question asked to respondents was: How often have you had to pay a bribe, give a gift or do a favor to: a teacher or school official; a health worker or staff member of a clinic or hospital; a government official to obtain a document; a government official to receive public services; a police officer; or a judge or judicial official; or have you never done so? Respondents who had occasion to make any arrangements for a service described in the previous 12 months, excluding missing responses.

Figure 1.1. **Percentage of people who have paid bribes in Latin America and the Caribbean 2017 and 2019.**



Source: Transparency International, Global Corruption Barometer 2017 and 2019 results.

How can an agenda that reduces corruption in a sustained and transversal way be developed? In 2015, for instance, Mexico accelerated its State's digital transformation by creating a single portal for federal government procedures which has contributed to reducing bribery across federal public procedures. The platform www.gob.mx is part of the National Digital Strategy that began in 2014, and represents a reframing of the relationship between citizens and government. The platform allows citizens to carry out online the most frequently requested procedures of the Federal Public Administration such as those relating to identity, education, labor, taxes and contributions, health care, trademark registrations, communications and transportation licenses, social programs and tourism registration. Thus, information from over 5,000 federal government sites has been centralized in a single, easy-to-access platform with a simple and intuitive design.

By digitalizing and simplifying procedures with the automation of administrative processes, governments can limit public authorities' discretion and reduce the number of interactions with citizens that enable corrupt behavior (Santiso, 2021).

The World Economic Forum (WEF) recognizes digital technologies as an important ally in transparency and integrity, and as a fundamental tool in the fight against corruption (Santiso, 2020). New disruptive technologies of the so-called Fourth Industrial Revolution (4IR), such as blockchain and artificial intelligence, generate innovations that show a significant potential for companies and governments to reduce corruption risks.

However, in and of themselves, digital technologies do not guarantee greater integration or better management of public administrations. Certain conditions and enablers are required for governments to take advantage of the opportunities offered by the digital transformation to strengthen public integrity. Proactive transparency policies, access to open data and its reuse within a clear digital government policies framework represent the minimum input to develop public policies that facilitate the development of corruption prevention systems based on data intelligence (Cetina, 2020a).

This chapter presents a set of enablers for the effective deployment of new technologies aimed at preventing, detecting and investigating corruption

In this sense, the digitalization agenda must go hand in hand with government proactive transparency policies to create the conditions for technology to be used effectively in the fight against corruption. **This chapter presents a set of enablers for the effective deployment of new technologies aimed at preventing, detecting and investigating corruption, as follows:**

1. **It addresses digital government policy**, particularly, the digitalization of public procedures and records, and the automation of administrative processes such as public procurement.

2. **Proactive transparency and open data are discussed.** Digitalizing government services and public records implies generating considerable number of datasets, and also requires citizens to be able to access information related to digitalized services and processes.

3. Finally, **datasets with a recognized use in terms of integrity are identified**, as well as some applications which by reusing data enable accountability and social control initiatives, and contributes to prevent corruption risks and improve public management.

1.1. Digitalization of government services and public integrity

In Latin America, at least before the COVID-19 crisis, citizens' interaction with their governments usually required going to a government office, queuing for hours to file a physical document, then requesting information on an issue, and interacting with public officials. In some cases, as shown by Transparency International, in-person processes meant exposing oneself to undue requests for payment to expedite government procedures. This scenario contrasted with civic life's progressive digitalization which involved the use of social networks to reveal consumer preferences, electronic platforms to pay for goods or services, to receive salaries, or the massive adoption of services such as e-mail and instant messaging for work.

Along the recent digital acceleration, progress has also been made in simplifying interactions between citizens and institutions. According to the Inter-American Development Bank - IADB (2018), before the pandemic, a Latin American citizen regularly took 5.4 hours to complete a procedure, with significant differences occurring between countries. However, digital services have contributed to accelerate public procedures (74% faster on average), and make them more efficient (for governments digital procedures cost between 2.35% and 5% less than face-to-face ones) and are a strategy accepted by citizens to improve public management (Roseth, Reyes and Santiso, 2018, p. 76). These efforts also contribute to the integrity agenda, because the procedures' complexity opens room for corruption and improper requests to citizens.

International experience confirms the benefits of digitalization in strengthening the integrity of public policies. In the case of Estonia, for example, as of 1994 public administration's digital transformation was boosted by promoting the *Principles of Estonian Information Policy* (e-Estonia, 2021). Consequently, since 2017, 99% of procedures and services can be performed online[3]. The appropriation of digital services by Estonians is high. In 2014, 80 million digital transactions were carried out in a country of only 1.3 million inhabitants (Goede, 2019). To access e-services, citizens have a **digital identity** card that uses *blockchain* technology to generate a unique identifier. e-Estonia allows operations such as digital identification and signature, popular voting, vehicle registration and health care, among others, to be carried out completely online (United Nations, 2020).

[3] Marriages, divorces and real estate transactions are the only procedures that require physical completion (Goede, 2019, p. 218).

Moreover, e-Estonia has significant economic benefits: it saves 844 years of work for each year of information exchange operations made through X-Road[4]. On this platform, each government agency manages its own data, and it is possible for authorized entities to access other government offices databases. Thus, to carry out any type of procedure before different public and private authorities', citizens must provide their data only once (e-Estonia, 2021). Additionally, big data generated through transactions is used by the National Statistical Office for public decision-making[5]. This policy has also impacted transparency levels, as citizens can access open, standardized and structured data (Estonian Cooperation Assembly, 2020).

The aim of government digitalization is to integrate digital technologies as an element of administrative modernization strategies in order to create public value (OECD, 2014; IADB, 2016). This involves transforming analog paper-based systems traditionally used to interact with citizens so that public services become more efficient, agile, are deployed more intelligently, and focus on citizens' needs (Santiso, 2019). For example, since starting its government's digitalization in 1996, estimates show Dinamarca saves EUR 296 million annually, has reduced paperwork processing time by 30% and increased its transparency levels by 96% (Digital Denmark, 2021). Denmark has the online portal borger.dk where, due to the articulation of national, regional and municipal public agencies, the majority of services offered by the Danish public sector can be found and accessed (United Nations, 2020; Digital Denmark, 2021).

Transforming analog paper-based systems traditionally used to interact with citizens.

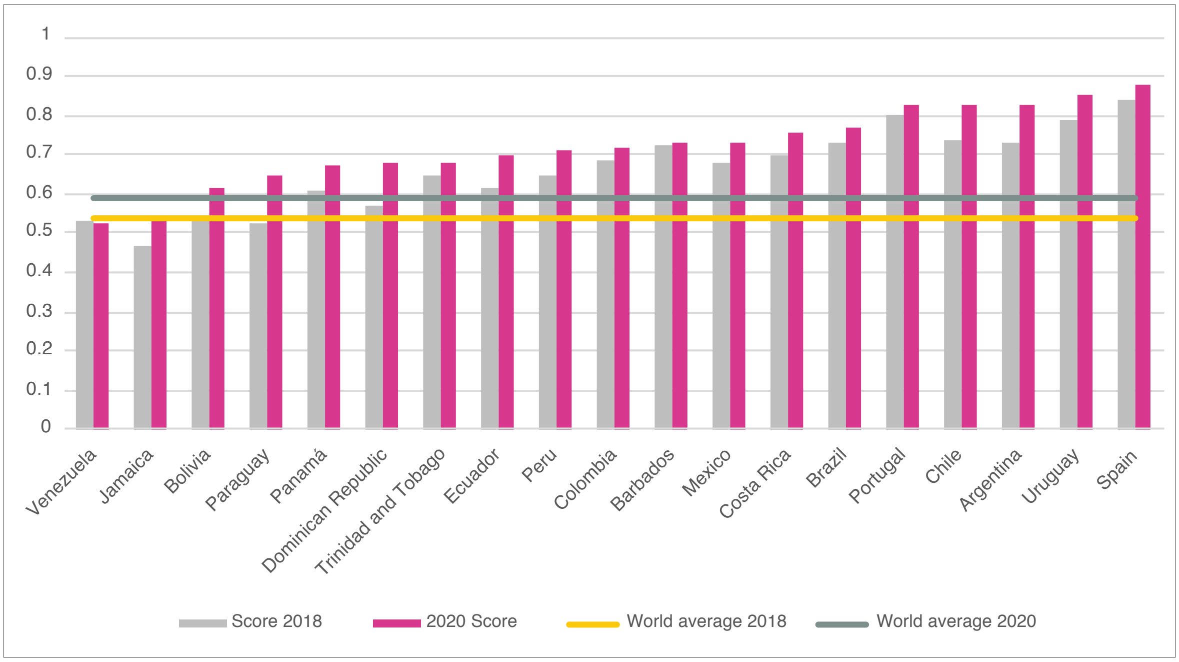
However, **digitalization is not limited to implementing technological platforms to carry out public procedures**. It also includes advances in digital connectivity and in citizen's digital proficiency. Government progress in digitalization is measured through the E-Government Development Index (EGDI), which is led by Denmark, Korea and Estonia. It is composed by three markers: digital services provision, telecommunications connectivity and citizen's digital proficiency. It is worth noting that, in 2020, 17 of CAF's 19 member countries placed above the global average calculated from the scores of 193 UN member countries included in the IDGE measurement (0.5988)[6] (see Figure 1.2). The variation showed in the index between 2018 and 2020 was mainly driven by an increase in the connectivity sub-index or *Telecommunication Infrastructure Index* (TII) that showed progress in telecommunications infrastructure in all CAF countries under measurement. With the exception of Peru and Ecuador, there was also an increase in the *Human Capital Index* (HCI) in almost all CAF member countries.

[4] Data exchange software that guarantees the accessibility, integrity and confidentiality of the data generated and required for the provision of public and private digital services.

[5] For example, cadastral data, real estate transactions, building permit applications, and data related to public transport use are big data that the Estonian government uses for transparent and evidence-based decision making (Estonian Cooperation Assembly, 2020).

[6] Jamaica and Venezuela, with scores of 0.5391 and 0.5268, respectively, were the two CAF member countries that were below the world average of IDGE in the 2020 measurement. It is noteworthy that, globally, the scores of Denmark (0.9758), Korea (0.9560) and Estonia (0.9473) are very close to the maximum of 1.

Figure 1.2. Resultados IDGE para los países miembros de CAF en 2018 y 2020

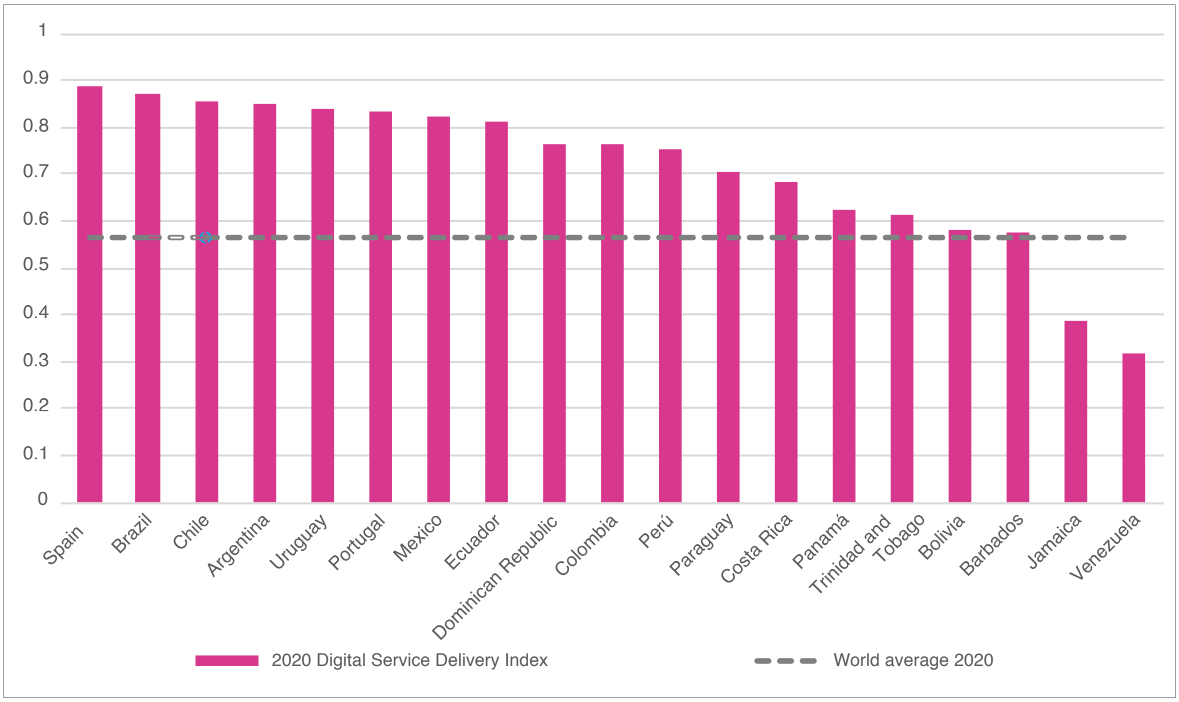


Source: UN (2020). The IDGE scale goes from 0 to 1, Denmark (0.9758), Korea (0.9560) and Estonia (0.9473) were the leading countries in 2020. The measurement assigns, to each member country, a score on a scale from 0 to 1, where 1 represents the highest level of digital government development (United Nations, 2020). The global average refers to the average score of the 193 countries included in the measurement for the years 2018 and 2020.

Development of online services offered to citizens is measured with the sub-index of digital service provision, *Online Services Index* (OSI), which is part of the EGDI. Here, CAF member countries show a behavior similar to that observed with this index. The rating's determinants include portal functionality, information availability, platform speed, intuitive portal design, the quality of the information provided and the possibility of executing online procedures (UN, 2020). In 2020, 17 of CAF's 19 member countries placed above the OSI global average (0.5262)[7] This measurement's leader was Estonia, with a score of 0.994, a country where 99% of procedures and services can be performed online (Figure 1.3).

[7] Jamaica and Venezuela, with scores of 0.3882 and 0.3176, respectively, were the only CAF member countries below the OSI world average in its 2020 edition.

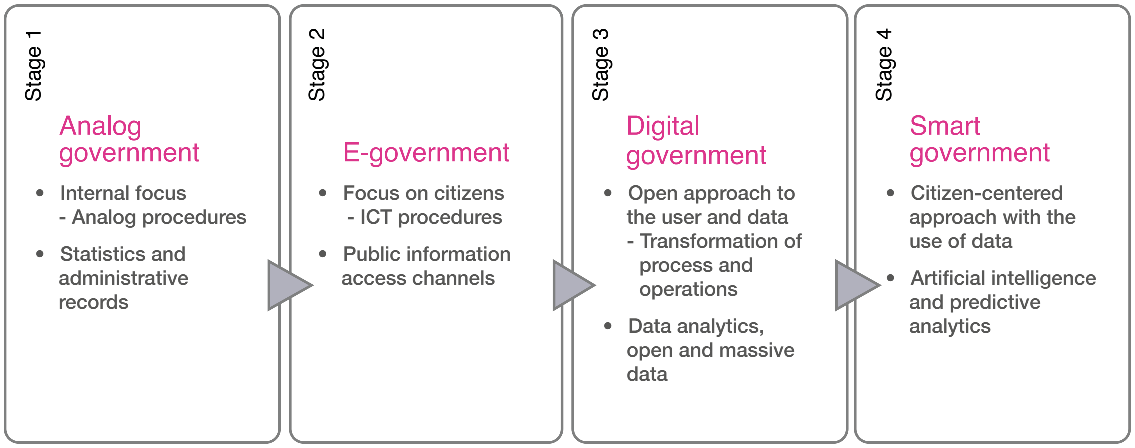
Figure 1.3. 2020 OSI results for CAF member countries



Source: UN (2020). The OSI scale ranges from 0 to 1; Estonia (0.994) was the leading country in 2020. The global average corresponds to the average score of the 193 countries included in the 2020 OSI measurement.

Governments digital transformation also involves harnessing data to improve public policies and service quality (Figure 1.4). There are four key capabilities for achieving smart government, i.e., guided by the use and reuse of data for predictive purposes e.g.; (i) digital services to citizens; (ii) internal administrative processes; (iii) data-driven administrative decisions; and (iv) the data itself, easily accessible and reusable, to enable digital innovation in public services (Santiso and Ortiz, 2020, p. 25).

Figure 1.4. Elements and stages of administrations’ digital transformation


Stage 1
Analog government
• Internal focus - Analog procedures
• Statistics and administrative records
Stage 2
E-government
• Focus on citizens - ICT procedures
• Public information access channels
Stage 3
Digital government
• Open approach to the user and data - Transformation of process and operations
• Data analytics, open and massive data
Stage 4
Smart government
• Citizen-centered approach with the use of data
• Artificial intelligence and predictive analytics

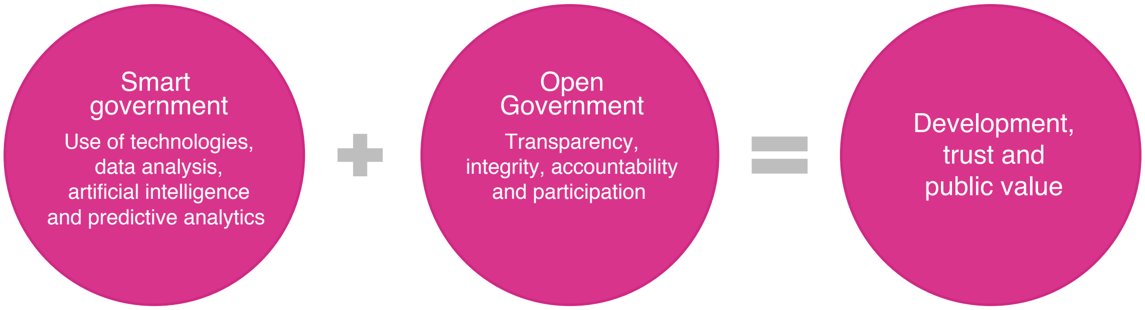
Source: Santiso y Ortiz (2020).

In addition to providing better services to citizens and saving public resources, the State’s digitalization makes it possible to centralize data containing information on the processes carried out by public administrations. When publicly accessible, these data and information, have the potential to foster higher levels of State transparency and integrity.

However, digitalization itself does not necessarily imply or generate higher levels of transparency, integrity and public value. Technology's potential is limited if the legal and institutional system does not enshrine the right to access public information or generate provisions on data openness (Volosin, 2015). Therefore, in terms of integrity, to really maximize digital systems it is up to governments to implement strategies and initiatives that enable access to public information and data reuse (OECD, 2021).

An initiative that articulates digital innovations, data and transparency within governments to enhance their effects on public policies is the **Open Government Partnership** (OGP), which started in 2011 with the Open Government Declaration. Through biannual action plans, OGP member countries, develop initiatives to: 1) increase the availability of information on government activities; 2) support citizen participation; 3) apply the highest standards of professional integrity; and 4) increase access to new technologies for open data and accountability. To date, most CAF member countries have adhered to OGP (OGP, 2021).

Figure 1.5. Enabling policies to strengthen development, trust and public value


Smart government
Use of technologies, data analysis, artificial intelligence and predictive analytics
+
Open Government
Transparency, integrity, accountability and participation
=
Development, trust and public value

Source: Own elaboration.

1.2 From access to information to proactive transparency with open data

In the last two decades, proactive transparency and open data have become key allies to fight corruption in the digital era. Mass, standardized and open data has facilitated the deployment of information analysis alternatives that would be impossible to implement using physical paper-based documents. Such analyses are only possible by adopting transparency and access to public information practices, which, like digital government, require a maturing process within government institutions and regulations, as proposed in Figure 1.6.

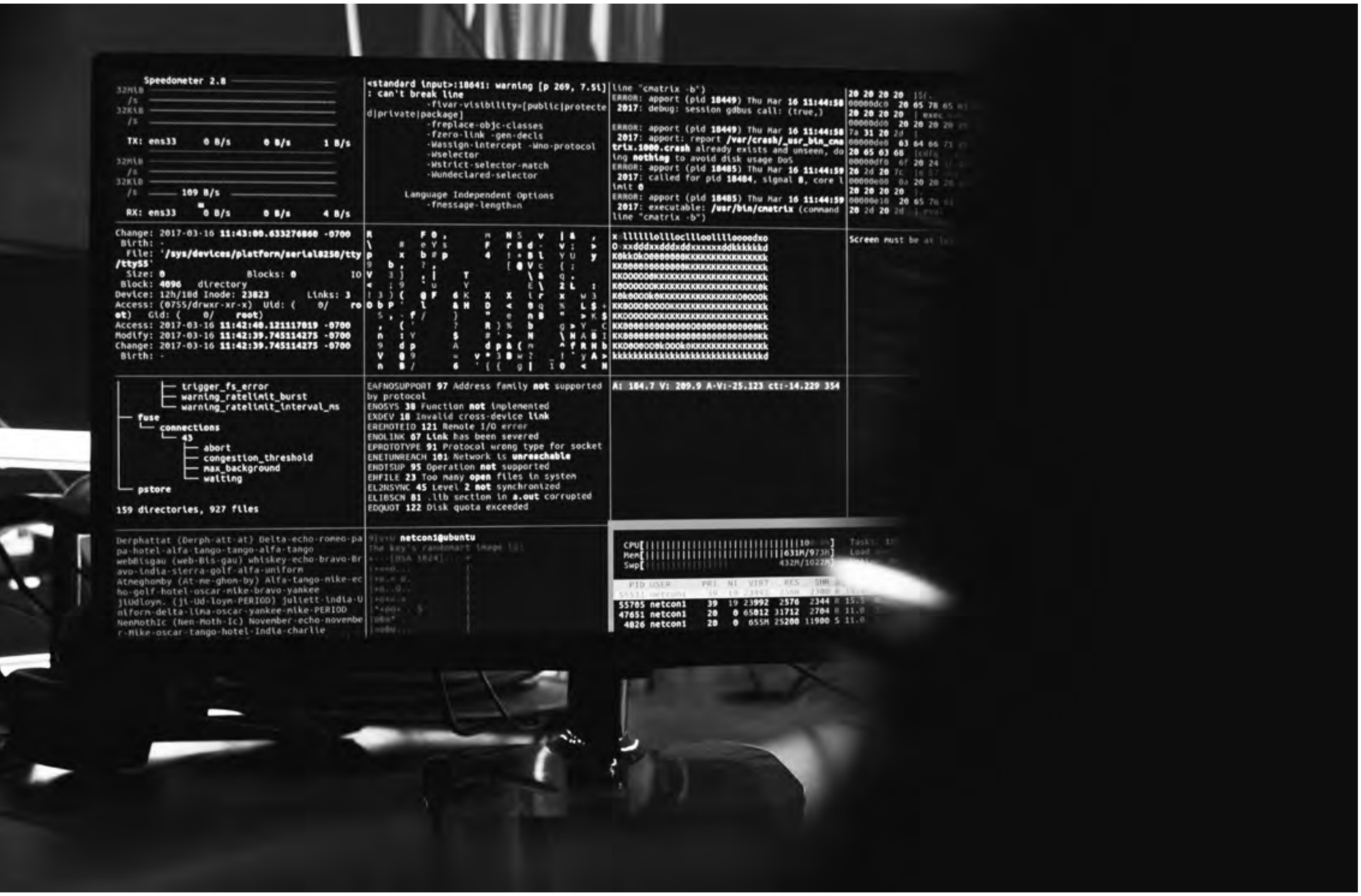
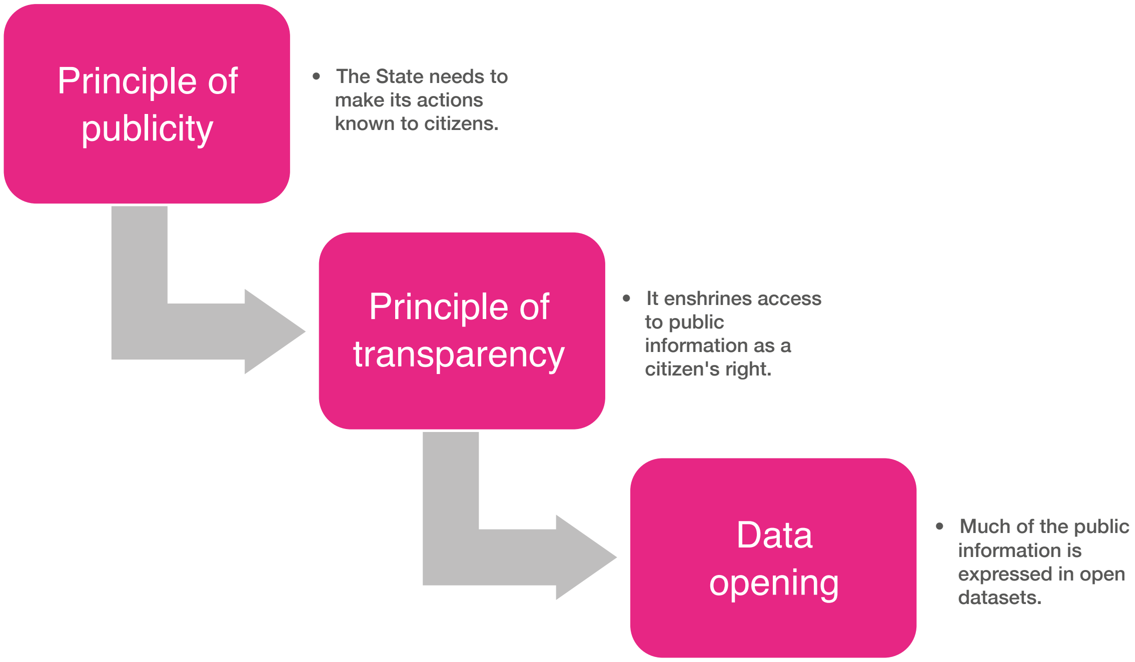


Figure 1.6. Evolution in access to public information


Principle of publicity
- The State needs to make its actions known to citizens.
Principle of transparency
- It enshrines access to public information as a citizen's right.
Data opening
- Much of the public information is expressed in open datasets.

Source: Own elaboration.

1.2.1 From the principle of publicity to transparency standards

The principle of publicity[8] **implies that the State's activities must be public. In other words, citizens should be aware of government actions, decisions, policies and the reasons behind them. In this sense, "grey areas"** where illegality or conducts that undermine the general interest can flourish should be evaded (Romeu and Rodriguez, 2013). Applying the principle of publicity also facilitates the development of public policies, since their formulation and implementation requires interaction between different actors; citizens; civil society; the private sector; public sectors (executive, legislative and judicial); independent agencies; and, supervisory authorities. Thus, publicizing the State's actions within the cycle of public policy is both a fundamental and a minimum requirement for their enforcement.

For public entities actions, the concept of transparency is more ambitious than that of publicity. The principle of transparency enables the exercise of

[8] In some countries of the region, such as Venezuela, the principle of publicity is called "principle of public accountability".

fundamental rights (due process, defense, access to public information and citizen participation), thus allowing control over authorities' decisions. Public knowledge and the channels of attention and interaction related to the government agencies' actions allow citizens to deliberate and claim their rights.

Free and direct access to data on government actions, and visualization tools that enable a much faster and intuitive understanding of the information, increases processes' transparency and strengthens public integrity.

Just as transparency goes beyond mere publicity, there are also access levels to public information. Therefore, we must distinguish between two types of government transparency:

- **Passive** refers to cases in which an interested party provides information as a result of a request or requirement to a public entity (De la Fuente, 2014). In this scenario, in exercise of the right to petition, verbal and written requests play a fundamental role. Petitions are requests submitted to public and private agencies in order to learn facts, demand documents, or ask for the provision or improvement of a service. Public entities must process and respond to them in a complete and substantiated manner within the existing legal framework.

- **Proactive** goes beyond merely responding to requests for information. It relates to government agencies' obligation to systematically, periodically and timely publish —without any requirement, all information and data not specifically subject to legal or constitutional reservations. That way, any individual, regardless of their status (citizen, foreigner, natural or legal person, adult or minor) and without the need to prove a particular interest or condition, has the right to access public data and information. Free and direct access to government actions data, and visualization tools that enable a much faster and intuitive understanding of information, increase process transparency and strengthen public integrity.

The regulation on access to public information in the region is several decades old. Nevertheless, due to the principle of proactive transparency, governments have been evolving towards open data (De la Fuente, 2014; ILDA, 2021). To this date, 18 CAF member countries, have regulations that guarantee access to public information (see Table 1.1). However, some of those regulations were issued over a decade ago and have yet to be updated. Therefore, many are not guided by the principle of proactive transparency and consequently, information can only be obtained through requests or requirements to public authorities. As can be inferred from the discrepancy between the adoption of transparency laws and the scarce acceptance of international standards such as the International *Open Data Charter* (ODC) there is a lag in terms of access to information in a world of massive data.

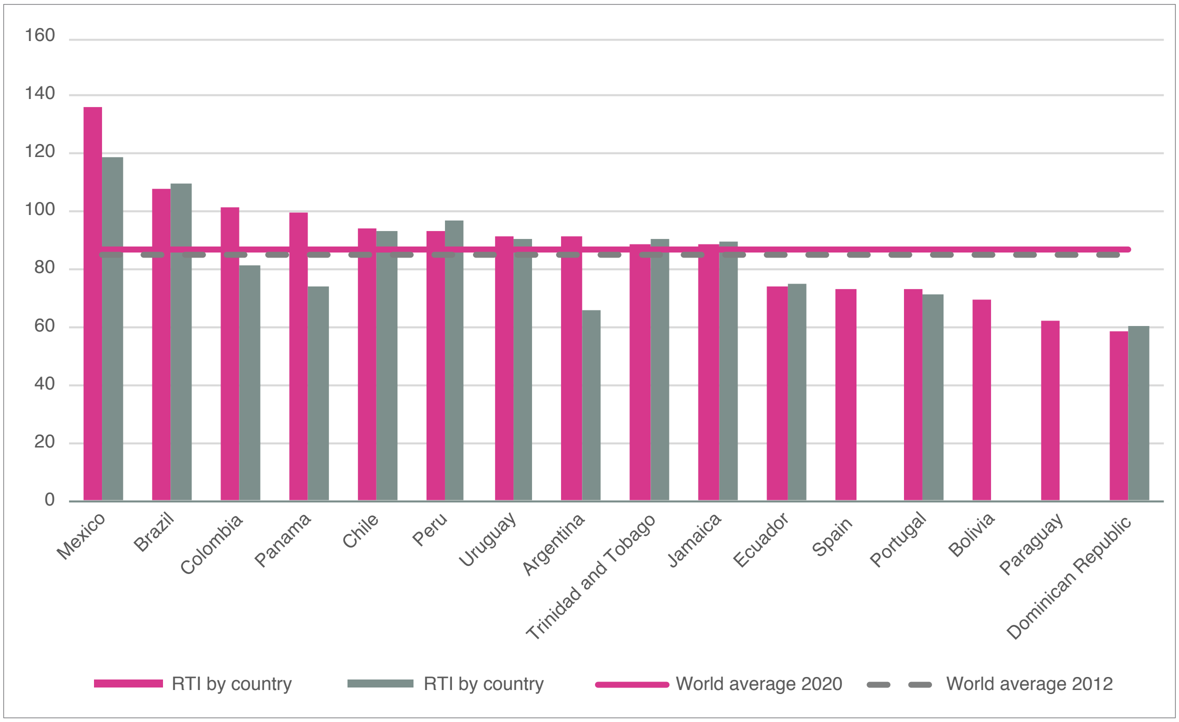
Table 1.1. CAF member countries' regulatory frameworks on access to public information

Country	Latest standards//N.°	Year	Open data policy	Open Data Charter Adopter
Costa Rica	Political Constitution (Articles 27, 30) - Executive Decree 40 199	1949/2017	✓	✓
Portugal	Law on Access to Administration Documents/ 65 - Law on Access to Administrative and Environmental Information and Reuse of Administrative Documents/26	1993/2016	✓	✗
Trinidad and Tobago	Freedom of Information Act/26	1999	-	✗
Mexico	Federal Law on Transparency and Access to Public Governmental Information	2002	✓	✓
Peru	Law on Transparency and Access to Public Information/27 806	2002	✓	✗
Jamaica	Freedom of Information Act/21	2002	-	✗
Dominican Republic	General Law of Free Access to Public Information/200-04 - Decree 486-12	2004/2012	✓	✗
Ecuador	Organic Law on Transparency and Access to Public Information/24 - Constitution	2004/2008	✓	✗
Bolivia	Supreme Decree on Access to Information/28 168	2005	✗	✗
Uruguay	Right of Access to Public Information/18 381	2008	✓	✓
Chile	Civil Service Transparency and Access to Information Law/20 285	2008	✓	✓
Brazil	Access to Information Law/12 527	2011	✓	✗
Venezuela	Organic Law of the Public Administration (Articles 9 and 13)	2011	✗	✗
Panama	Law creating the National Authority for Transparency and Access to Information/33	2013	✗	✓
Spain	Law on Transparency, Access to Public Information and Good Governance/19	2013	✓	✗
Colombia	Law on Transparency and Right of Access to Public Information/1 712	2014	✓	✓
Paraguay	Law on Free Citizen Access to Public Information and Government Transparency/5 282	2014	✓	✓
Argentina	Access to Public Information Law/27 275	2016	✓	✓

Source: Own elaboration based on De la Fuente (2014), ECLAC (n. d.), ODC (2021).

In addition to a citizen's right, access to open data represents an instrument to monitor and control possible corruption cases. Measurements such as the Global Right to Information Rating **RTI**[9] (see Figure 1.7) showed improvements in the quality of de jure standards of information access. However, there is still need to improve or streamline the procedures to request information and the imposition of sanctions for public officials who deliberately undermine the effective exercise of this right.

Figure 1.7. **Information access index (IAR) for CAF member countries 2012 and 2020**



Source: RTI 2019 and 2012. The RTI scale ranges from 0 to 160. A score close to 160 shows greater strength of legal frameworks. The global average corresponds to the average score of the 128 countries included in the RTI measurement in 2019, and 93 countries included in 2012.

Proactive transparency is an indispensable instrument in the public integrity agenda (Zapata, Scrollini and Fumega, 2020). Without the mediation of a verbal or written request and a bureaucratic process, individuals can

[9] Global Right to Information Rating (RTI), proposed by the Center for Law and Democracy and the Access Info team. It measures the strength of the legal framework for the right of access to information held by public authorities, taking into account 61 discrete indicators organized into 7 main categories: right of access, scope, application procedure, exceptions and refusals, appeals, sanctions and protections, and promotional measures (RTI, 2021).

access complete and updated data on government actions in a format that enables its reuse for analytical purposes. For instance, prior tothe existence of e-procurement platforms, knowledge of public procurement data implied overcoming a series of barriers: tendering an information request, submitting to internal procedures, and waiting to receive non-standardized or obsolete data. With the evolution of digital platforms containing open data in real-time (which even allow the creation of intuitive visualizations, as in the case of Paraguay), knowledge, participation and control over public actions is stricter and more informed.

1.2.2. From proactive transparency to open data

Open data is transparent, accessible and can be reused for analytical purposes through automated tools. The Open Knowledge Foundation (OKF) defines open data as data that people can use, reuse and redistribute freely, without legal, technological or economic restrictions. The OCDE defines open data as data that is available, accessible and reusable without government-imposed barriers (i.e., machine-readable). In 2015, awareness on the importance of presenting public information in open data format to facilitate and enhance its reuse began to grow. The United Nation's National Assembly enacted the Open Data Charter (ODC), establishing fundamental principles to support transparency, innovation and accountability in public data governance. The charter highlights the importance of data in gearing governments' transformation towards greater transparency, efficiency and effectiveness. The principles set out in the ODC are described in Table 1.2.

Table 1.2. Principios para la apertura de datos gubernamentales

Principio	Contenido
Default opening	The general rule is that all government data must be publicly available, except when there is an explicit and justified legal reason. Moreover, access to data should not compromise the user's privacy. For example, governments should keep available data on the procurement of medical supplies during the pandemic. However, regulations may expressly and exceptionally state that some data is subject to confidentiality. This is the case, for example, of industrial secrets (chemical components of vaccines), or others related to "national security and national defense" (military intelligence reports).
Timely and complete	Data should be timely published, be complete, untampered and updated periodically. This implies that, for example, data from a contractor selection process should be made public in a timely, complete and untampered way before and not after the procurement process has been completed.
Accessible and usable	There should be no administrative, economic or technological entry barriers. Portals should facilitate user experience, allow access without user registration, provide access and download formats that maximize usability, and be completely free of monetary charges.
Comparable and interoperable	Data should be standardized to allow comparisons and integration with other datasets and systems. In this sense, for instance, data that a national public procurement agency has available on its web portal should comply with standards that allow any interested party to compare it with other sources, such as, for example, control bodies websites.
To improve governance and citizen participation	Data should enable citizens, private sector, civil society and government agencies to learn about public sector performance. Transparency and accountability improve the provision of public services, enable oversight of State agents and the rule of law.
For inclusive development and innovation	Access to data opens room for innovation opportunities. It also offers greater societal and economic benefits.

Source: ODC, 2015.

Open data allows governments to trace their actions and interactions to identify irregularities, disclose them, correct them, prevent them and/or sanction them. For this to be possible, governments must overcome three general limitations that make it difficult to take advantage of datasets (Cetina, 2020a; ILDA, 2021; ODC, 2018):

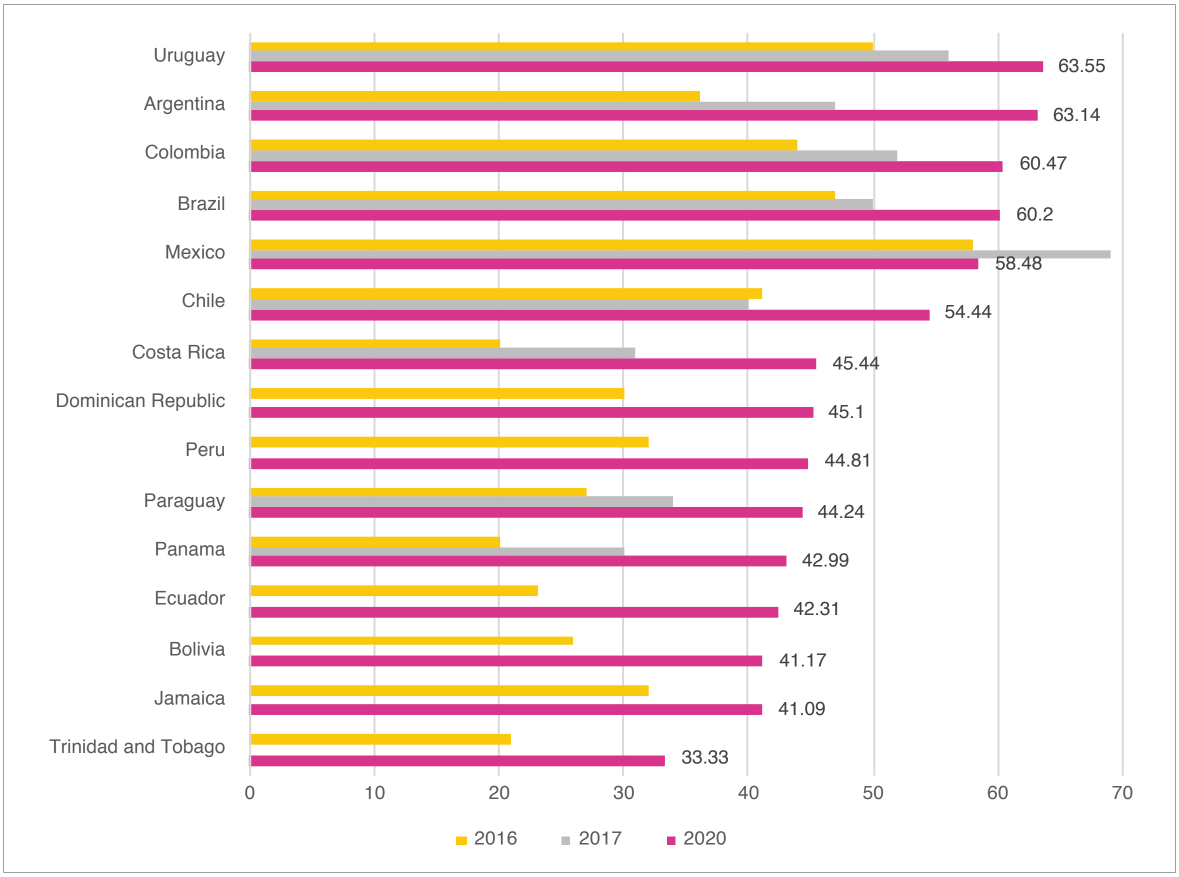
- **Availability:** data must exist and be produced in such a way that it can be used, reused and distributed without restrictions.
- **Integrity:** data must capture information that reflects reality in a way that is accurate, complete, homogeneous and consistent with its creators' intentions. Therefore, countries must design information systems that work to record facts and data and to ensure the information's accuracy and the uniformity with which it is digitized.
- **Structure:** databases must have a predefined internal structure (organization and formats) that facilitates interoperability between different systems. When data is not structured, it generates difficulties for use, reuse and distribution (i.e., e-mails, texts in social networks, audios, videos, flat text files and PDF formats).

According to the Regional Open Data Barometer for Latin America and the Caribbean 2020 (ILDA, 2021), which measures the readiness[10], implementation[11] and impact of open data[12], the region showed marginal growth compared to its 2016 results, achieving an average score of 40.38 on a scale of 0 to 100. This reflects a slowdown in the agenda, particularly in the areas of

[10] Refers to the willingness of governments, citizens and entrepreneurs to ensure the openness of data.
[11] Corresponds to the degree to which governments publish key Datasets in an accessible, timely and open manner.
[12] Identifies the extent to which there is evidence that the publication of open government data has had a positive impact on a variety of sectors in the country.

preparation and impact. Progress in implementation is uneven, and in terms of impact, observed countries did not show much progress (Zapata, Scrollini and Fumega, 2020).

Figure 1.8. **Results of the Regional Open Data Barometer for Latin America and the Caribbean for CAF member countries in 2016, 2017 and 2020**



Source: Zapata, Scrollini and Fumega (2020). The scale ranges from 0 to 100, a score of 100 shows higher levels of readiness, implementation and openness. The United Kingdom is the leading country with a score of 76.

In order for open data to move forward, the Latin American Open Data Initiative 2021 (ILDA, by its Spanish acronym) recommends that the region's governments:

i) invest in a constant and sustained manner in teams that guide and implement open data policies at all levels of government;

ii) implement a holistic view of data, including regulatory aspects of privacy protection, uses for the common good and inclusion of vulnerable populations;

iii) increase efforts to include the private sector and civil society in the open data ecosystem;

iv) generating better and greater data uses to produce benefits for various groups in society, and

v) promotes political support for the open data agenda.

In general, adoption of proactive transparency and citizen-centered digital government standards precedes the open data agenda, this way the latter can acquire purpose and capture relevant information. In this process, the most important datasets for the integrity agenda and for the fight against corruption are being shaped through their publication and reuse, as illustrated in the following section.

Box 1.1. Open information portal on public procurement in Ecuador

At the end of 2021, the Open Information Platform for Public Procurement was launched as a result of the cooperation between CAF, *Open Contracting Partnership* and the support of the Ministry of Telecommunications of Ecuador (MINTEL, by its acronym in Spanish).This initiative was built in compliance with open government commitments by the National Public Procurement Service (SERCOP by its acronym in Spanish). SERCOP is the governing body of the National Public Procurement System (SNCP by its acronym in Spanish), responsible for the development and management of the Official Public Procurement System of Ecuador (SOCE by its acronym in Spanish) and for establishing policies and conditions for public procurement at the national level.
This tool's, implementation is expected to improve the dissemination, use and quality of public procurement data by the different actors within the National Public Procurement System (SNCP). By the end of 2021, the platform has registered at least 127,163 procurement procedures, which represent a total amount of USD 3.6 billion in awarded contracts. The portal also allows browsing according to characteristics such as type of contract, associated sector, entities, companies and contract amount.

Source: Own elaboration.
Source: CAF (2021).

1.3. The role of open data in integrity policies

1.3.1. Datasets to fight corruption

Access to public information linked to digitalization and the fourth industrial revolution's acceleration allowed governments to organize their information into better structured data to facilitate its reuse with specific purposes. The recognition of access to public information as a right opened room for citizens to demand information on the decisions and actions of public institutions.

Specific datasets useful for public integrity vary according to investigated behaviors and the nature of the agency interested in preventing,

detecting and investigating corruption. In fact, within the data ecosystem used by governments, there are efforts to identify and to make key information for the fight against corruption, such as the ODC's Open Data Guide, readily accessible and reusable[13].

This report highlights six datasets that have shown great capacity to raise early warnings on corruption risks and vulnerabilities in integrity systems. Among others, these risks relate to relationships, communications, locations and patterns behind certain public decisions and government transactions, according to the uses that will be shown in chapters 2 and 3.

1. **Contracting and public procurement data:** today, it is possible to access information related to the different stages of government procurement processes from the moment a supply need is identified to the final delivery of goods and services. Among others, the main variables related to these State processes are; supply conditions; purchasing prices and quantities; bidders' nature and names; companies or individuals awarded contracts; addenda; renegotiations; penalties and compliance records; and, execution reports. In Latin America, the portals for the public procurement and contracting agencies of **Buenos Aires**, **Chile**, **Colombia**, **Uruguay** and **Paraguay** have implemented the (*Open Contracting Data Standard* (**OCDS**). This records and allows open data consultation on the most important variables in pre-contractual, contractual and post-contractual stages of each procurement process. However, it is important to mention that each country's laws establish limits for disclosure of public information in cases such as those related to industrial and commercial secrets, national security and national defense. These limits must be evaluated on a case-by-case basis without governments being able to generically classify certain information as secret based on these limitations (IACHR, 2020).

2. **Declarations of assets and interests[14]:** although there is no international standard in this area, generally, these are documents signed by public officials to indicate the existence of private interests that could conflict with their exercise of public office (CAF, 2019). In most regional countries, public officials[15] must declare to the authority that regulates and supervises civil service the nature of their assets, debts, savings accounts, securities, and membership in boards of directors, assemblies or councils in private legal entities. Generally, thesedeclarations must be made yearly, and constitute

[13] See https://opendatacharter.net/themes_and_topics/anti-corruption/

[14] Declaring assets and interests is the same act and requires the same format, since ownership of certain assets may generate a conflict of interest. Think of the shareholding that an official has in a company that contracts with the State, or the ownership of real estate whose value may be affected by a public intervention, such as the construction of roads or the authorization of licenses for land use.

[15] Generally, this information should be filled out by management level officials with direct responsibility for decision making in public authorities or public companies, as well as others with advisory functions for decision makers.

The Office of the Comptroller General of Peru has a platform that the public can use to download multiple public authorities' statements at a time.

the first lines of defense against possible conflicts of interest[16] that exist in the exercise of public office. In France, for example, the Transparency and Public Information Authority gathers and publishes declarations of assets, income and conflicts of interest through its portal **www.hatvp.fr**. In Mexico, the platform **Declaranet** allows inquiries into the assets and income declared by public officials in .csv[17]format. In other countries, such as Paraguay[18] this information can be accessed as long as a request is made to the Comptroller General's Office. Similarly, the Office of the Comptroller General of Peru has a platform where the public can download multiple public authorities' declarations at a time.

3. **Tax data[19]:** By nature, tax authorities have privileged access to information on taxpayers' addresses and movements. They also need to capture structured data to manage their own tax collection information. For example, in Argentina, the National Tax and Social Identification System (**SINTyS**, by its acronym in Spanish) integrates and links individuals and companies' data in the cloud in real-time to reduce evasion and control informality. Chile's Internal Revenue Service (**SII**, by its acronym in Spanish) captures so much data on taxpayers that it generates pre-filed returns with information obtained from banks and taxpayers economic transactions[20].

4. **Company registrations:** Formally registering legal entities, particularly companies or firms, is a necessary step to incorporate and recognize them before the State and third parties in the market. Information underlying different types of companies and corporate vehicles such as assets, shareholders, governing bodies members, legal representation and beneficial owners as well as the relationships between parent companies and subsidiaries, is generally managed and centralized by entities in charge of publicly attesting to such records. For example, in Colombia the Single Business Registry (**RUES**, by its acronym in Spanish), gathers information from all chambers of commerce allowing citizens the possibility of open consultation as long as they have the tax identification number of the company they want to investigate.

5. **Sanctions for natural and legal persons:** Judicial authorities are empowered to condemn corrupt practices, such as bribery or the improper attribution of contracts, and to generate records on such actions. For their

[16] This type of data may not be fully available for public consultation, since it contains personal information fields (addresses, account numbers), and is therefore considered reserved under access to information laws or protected by personal data access laws. However, they are very useful in administrative or judicial proceedings.
[17] See http://servidorespublicos.gob.mx/registro/consulta.jsf
[18] This type of data may not be fully available for public consultation, since it contains personal information fields (addresses, account numbers), and is therefore considered reserved under access to information laws or protected by personal data access laws. However, they are very useful in administrative or judicial proceedings.
[19] See footnote 15.
[20] Seco and Muñoz. (2018). Overview of the use of innovative digital technologies and solutions in fiscal policy and management. Working paper, Washington, D.C.: IADB. Available at: https://publications.iadb.org/publications/spanish/ document/Panorama-del-uso-de-las-tecnolog%C3%ADas-y-soluciones-digitales-innovadoras-en-la-pol%C3%ADtica-y-la- gesti%C3%B3n-fiscal.pdf

part, some administrative authorities may punish conduct such as collusion or cartelization, which are of particular concern in public procurement. Data on the criminalization of corruption or money laundering is essential to identify certain patterns —repetitive behaviors, convictions or fines averages, locations where crimes are committed, etc., and to better understand the nature of corruption. Such records are also necessary to enforce prohibitions or restrictions on those sanctioned to do business with the State or private individuals.

6. **Financial intelligence data[21]:** Currently, 17 Latin American countries are members of the Financial Action Task Force of Latin America (**GAFILAT**, by its acronym in Spanish), the regional version of the Financial Action Task Force (FATF) mandated to prevent and combat money laundering. GAFILAT has generated recommendations to consolidate Financial Intelligence Units (UIF, by its acronym in Spanish), as well as regional judicial cooperation to investigate an punish money laundering crimes. Information management measures like the Suspicious Financial Transactions Report (STR) or the distinction of Politically Exposed Persons (PEP)[22] help to consolidate information that makes it possible to follow up on transnational operations, understand their patterns and identify risks that, in many cases, are associated with corruption.

These datasets are an important input to identify improper practices and corruption risks, and are based on three types of analysis: descriptive, preventive or prescriptive (Cetina, Fonseca and Zuleta, 2021). Digital innovations seek to overcome reactive roles and adopt more proactive ones such as prevention motivated by the ability to predict in the fight against corruption. In a reactive role, the stakeholder's focus —business, government and civil society— is on detecting, disclosing and sanctioning acts after corruption and its damage have materialized. In the proactive role, improper actions are identified early, and corruption can be prevented before the State's assets are damaged and public interests are affected.

[21] This information also has restrictions on public access. It may be classified or reserved, thus falling under the exceptions to the principle of publicity existing in the access to information laws.

[22] See Financial Action Task Force of Latin America https://www.gafilat.org/index.php/es/gafilat/preguntas-frecuent

Table 1.3. Data use purpose

Descriptive	Preventive	Prescriptive
Analysis of cluster associations to identify behaviors, problems and opportunities.	Statistical modeling and regression to detect patterns, make projections and identify risks.	Simulation and optimization techniques to evaluate decision alternatives.
Graphs, histograms, pie charts and interactive visualizations to understand what happened in the past.	Structured data analytics to understand what is likely to happen.	Structured data analytics to understand what needs to be done.
Descriptions or diagnoses of expenditures, categories of goods, works and services, selection methods, etc.	Forecasts to support spending efficiency and potential corruption risks.	Prescription of solutions to optimize resources, improve operations and anticipate process difficulties.

Source: Cetina, Fonseca and Zuleta (2021).

1.3.2. Specific contributions of open data in the fight against corruption

It is possible to highlight some ways in which digitalization and open data have been used to achieve higher levels of integrity by enabling accountability and social control initiatives.

An example in terms of **accountability** is the *Construction Sector Transparency Initiative* (**CoST**) which allows citizens to interact with government and private sector entities and to access information on public infrastructure investments by publishing key data related to the occurrences at each stage of the project. In a web environment, CoST is responsible for geo-referencing infrastructure projects information, publishing open data on different projects, the contracts that comprise them, the resources invested and its potential beneficiaries. In Latin America, countries such as Argentina, Colombia, Ecuador and Panama are adopting this initiative.

Box 1.2. CoST Platforms for Jalisco (Mexico) and Bogota (Colombia)

In 2020, CAF supported the development of **CosT platforms for the state of Jalisco**, Mexico, and the city of Bogota, Colombia.
Following the Open Contracting Manual for Infrastructure Open Contracting Manual for (**OC4IDS**) guidelines, CoST platforms publicize information on key development infrastructure projects on these territorial entities.
In the case of Jalisco, data is published on 37 projects, including urban renewal, sewerage and roads with an allocated budget of more than US$500 million.
In Bogota, the aim is to ensure transparency and accountability in projects valued at USD 7.3 billion such as the construction of the city's first subway line, hospitals, wastewater treatment and road networks (Infrastructure Transparency Initiative, 2021).

Source: CAF (2021).

As mentioned, another area where open data, its consultation and use have a practical application for integrity is the exercise of *social control*, especially from initiatives promoted by *Civic Tech and GovTech startups*. Data-driven technologies aim to reinvent public sector practices, provide new capabilities and increase citizen and businesses trust in State agencies. GovTech companies are a bet on solving public problems by developing digital innovations that reuse data (Santiso and Ortiz de Artiñano, 2020).

For example, Datasketch, a Colombian GovTech startup that provides solutions to use, visualize and download information on the strengthening of public management through an intensive use of data and new digital technologies (Cruz, 2020) developed the **Citizen Corruption Monitor** platform. In 2018, with support from the United Nations Development Program (UNDP), the Ministry of Information and Communication Technologies (MinTIC, by its acronym in Spanish), and the Somos Más organization, developed the Elections and Contracts platform with the objective of enabling analyses on the relationship between electoral campaign financing and public procurement data. In 2019, Citizen Monitor's third phase was launched, which allows consultation of open and public data on corruption in Colombia. It is based on corruption cases reported by the press, the systematization, categorization, validation and publishing of data in four sections; general information (type of corruption, department, sector and entity); characteristics (year, type of investigation); consequences (impact in population groups and amount of money involved); and, acts. Until 2020, the platform identified and systematized 967 corruption cases concentrated, among others, in the defense and security (20.79%), judicial (11.17%), education (9.31%), housing (8.07%), health (6.93%), transport

(6.41%) and electoral sectors, adding up to an approximate value of COP 92.77 billion (Transparency for Colombia and Citizen Corruption Monitor, 2021). In a recent study to calculate the Citizen Monitor platform's cost-benefit, CAF concluded that every dollar invested in this digital development has a return of 37 dollars (Cruz, 2020).

Digital technologies based on data seek to reinvent public sector practices, bring new capabilities and increase citizen and businesses' trust levels in government agencies.

In Argentina, the startup GovTech Munidigital founded in 2015, facilitates citizen control over local government actions (10 provinces and 50 municipalities) and provides digital solutions for some members of the Argentine Network of Municipalities against Climate Change (RAMCC, by its acronym in Spanish). In addition to managing public tree lining interventions, the MuniArbol software contains data on tree species, images, age, condition and geopositioning. The app detects irregularities, shortages and risks in the provision of vegetation in localities (RAMCC, 2020). In another collaborative effort to reuse open data in the pandemic's context, the municipality of Villa Carlos Paz, which has approximately 62,000 inhabitants, used MuniSocial as a tool to organize, prioritize and geolocate social assistance. The database created from MuniSocial contains details on the families receiving aid, —which may be governmental, provincial or municipal, with specific individual's data and specific validated requirements. This application allowed aid to reach the most vulnerable people and to create a map of vulnerable areas (Santiso, 2020; González, n. d.).

1.4. Closing remarks: consolidating an agenda for data for integrity

Open data and governments digital transformation gained and unprecedented importance for the world during the health and economic crisis caused by COVID-19[23]. Digital acceleration also represents an opportunity to fight against corruption, provided it is supported by public policies that ensure proactive transparency and open data with the potential to generate a corruption risk alerts.

Data proliferation and reuse allows new technologies to become part of the public integrity agenda. However, **for this digital transformation to be successful in anti-corruption matters, it requires institutional and technological adjustments in governments based on the following four pillars:**

1. **It is necessary to adopt reforms and practices that guarantee proactive transparency in government authorities**, publishing all information that is not specifically subject to legal or constitutional reservations, without the need for petitions, administrative or judicial procedures.

2. **To adopt successful open data policies proactive transparency must be articulated and coordinated with digital government agendas.** As processes within governments and citizen procedures are digitalized, mechanisms should be developed to open produced data to the public, as is the case with public procurement. This can be extended to other matters, such as license issuance, digitalization of conflict-of-interest declarations and records for companies and their beneficial owners. This should ensure standards of quality, structure and reusability for the data made generally available in each matter as regulated by laws on access to public information.

3. **Once the open data policy ensures a robust data infrastructure (quality, integrity and reusability), data reuse allows to understand and prevent complex phenomena such as corruption.** Moreover, transparency regarding government actions and management generates a higher level

[23] Large datasets, duly shared and reused, helped us to be certain about the circumstances of the appearance of the virus among humans: the illegal market of exotic species in the city of Wuhan, China. It is even more astonishing to know that corruption phenomena associated with organized crime enabled the appearance of the virus, since it was in the midst of the illegal trade and slaughter of species that COVID-19 managed to pass from animals to humans, giving rise to the pandemic and opening a new era for the planet. In a kind of spiral, this crisis accelerated the digital transformation of economies and governments, giving data a more fundamental role as an asset for the management of States and the functioning of markets.

of trust among citizens. Low-cost access to critical data creates a basis to develop applications and platforms that respond to citizens' needs, improve State management by evaluating it through analysis and cross-referencing of large datasets, and facilitates government accountability.

4. **With a consolidated open data agenda, governments can advance in the adoption of internationally recognized standards in areas of special interest for public integrity,** such as procurement, taxation, public spending, infrastructure and civil service. The application of international standards and practices to produce, publish and reuse data is a cost-effective alternative to provide useful information for anti-corruption programs and initiatives. For example, adopted by the 2018's Summit of the Americas, the Inter-American Open Data Program (PIDA, by its acronym in Spanish) against corruption contains a set of recommendations to leverage 30 datasets that can be used in the fight against corruption.

Governments in the region are undergoing digital transformation processes. If properly oriented, these can promote development, trust, integrity and public value (Santiso, 2020). The COVID-19 crisis accelerated this process and placed the need to advance digital transformation and promote integrity policies at the center of governments agenda. New developments in information and communications technologies, accompanied by an open data policy, contributed to the battlefront against the coronavirus, and also have the potential to help in the fight against corruption.

2. A closer look to the evidence on the link between digitalization and integrity

“

—[…] It is a capital mistake to theorize before one has data. Insensibly one begins to twist facts to suit theories, instead of theories to suit facts.

Sir Arthur Conan Doyle, Scandal in Bohemia, in The Adventures of Sherlock Holmes

A closer look to the evidence on the link between digitalization and integrity

During the last decade of the 20th century, **e-government gained traction due to the need to implement technological solutions that modernized public management**, improved citizen government services provision and empowered private sector and civil society through greater transparency and access to information (OECD, 2003; World Bank, 2015). Independently and in parallel, the fight against corruption began to require coordination mechanisms between countries: in 1996, with the **Inter-American Convention Against Corruption**; in 1997, with the **OECD Anti-Bribery Convention**; and in 2003, with the **United Nations Convention Against Corruption**. Each of these conventions, encouraged proactive transparency and recognized the role of technology and data in the adoption and monitoring of measures to prevent corruption (see Chapter 1).

In the public finance sector, the relationship between transparency and e-government policies started to become evident at the beginning of the 21st century. First, government databases had to be ordered so as to present public accounts and access international credit. The impulse given to governments by international lending agencies to adopt standards in the organization and structure of public finance data was decisive because it opened room to design control spending measures, detect inefficiencies and improve investment. In public finance, e-government was gaining ground hand in hand with Information and Communications Technologies (ICTs), particularly in the administration of social security and social plans (which multiplied after 2000), and in fiscal transfers to subnational levels.

Thus, almost by chance, two international trends from different ecosystems aligned: i) that of international conventions that began to promote the adoption of transparency and public integrity measures among governments, and ii) that of the government which found in ICTs a means to organize and disclose information concerning its fiscal management and results.

In 2009, the agendas of technological integration and transparency in public policy began to intertwine more clearly. That year, a U.S. presidential memo coined the concept of **open government**, which promoted an initiative for government management based on transparency, collaboration, participation and digital innovation. This turning point would lead to the formation of the Open Government Partnership. This way, **the transparency agenda began synchronizing with the transition from analog to digital governments, thus turning technology into a decisive tool for the concept of** open government, in which information and communication permeate the administration of public organisms and facilitate their interactions with citizens.

Towards the second decade of the 21st century, the acceleration of data production and its massive processing for decision making, predictions and public spending correction, allowed governments to implement public data **repositories to improve their public management's monitoring** (IADB, 2016). This evolution implied going beyond the simple introduction of digital technologies in public management; instead, they had to be fully incorporated to produce a true modernization of the public sector, that executed processes and provided citizen-centered services (Santiso and Ortiz, 2020).

Although gradually, the processes of digitalization and the fight against corruption are interrelating in the area of public management. However, literature on the subject has not documented the dynamics behind this link with the same abundance.

Although gradually, the processes of digitalization and the fight against corruption are interrelating in the area of public management. However, literature on the subject has not yet documented the dynamics behind this link with the same abundance. One group of findings is restricted to linking specific digitalization cases with either the prevalence or reduction of corruption. For example, Andersen, Bentzen, Dalgaard, and Selaya (2010) argue that the internet is a powerful anti-corruption technology and also an important driver of economic growth. Haafst (2017) shows evidence suggesting that it is not the internet or digitalization that influences corruption, but rather the bureaucratic procedures that underly digitalization itself. Bologna (2014) discusses the concept of digital literacy and suggests that there is a negative correlation between digital literacy and corruption. Finally, Bailard (2009) supports that idea through cell phone use, and states that the decentralization of information decreases the opportunities for corruption.

Choi's seminal work (2014) addressed the concept of *e-Government* more comprehensively and found positive effects on corruption reduction. The author used the e-Government Development Index (e-GDI) results and the sub-indexes of telecommunications infrastructure and citizen's online activity and concluded that these areas have a statistically significant influence on corruption. In particular, that work suggested that governments enable access to information, open room for accountability and empower its citizens to interact with them.

However, over the last ten years, digital acceleration has affected the way that public institutions provide services and the scale for reusing large datasets. This suggests that the relationship between digital governance and integrity offers more properties that should be considered to formulate and implement integrity policies. This chapter documents some properties of digital governance, as follows:

- **The first part presents an analysis of statistical evidence exploring the relationship between digital government and integrity and digital government's proven effects in reducing corruption** within sectors that are particularly sensitive to public finances (*i.e.*, public spending and investment, internal control, public procurement and customs).

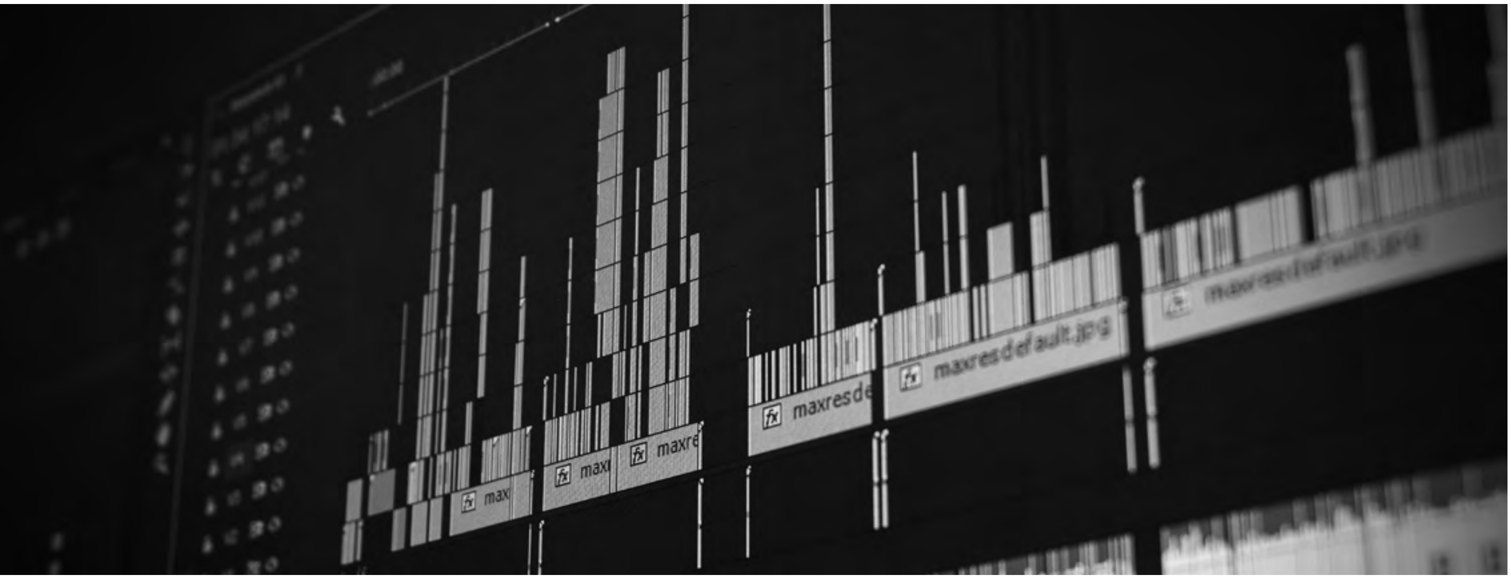
- **The second part describes Latin American experiences, where the expansion of digital government policies and services has paid integrity dividends.** From a qualitative standpoint, this segment analyzes specific national experiences on three operational fronts: procedures, public procurement and citizen participation.

- **At the end, the chapter reflects on the evidence presented and the lessons offered in terms of digitalization and public integrity.** Generally, we observe that academia, public sector and civil society still need to join efforts to identify the most effective digitalization strategies in the fight against corruption. This implies adopting data reuse practices in government digitalization initiatives for the purpose of evaluating public policy, as an integral part of the government's digital policy cycle.

2.1. A review of statistical evidence on the relationship between digital transformation and corruption

Technology plays an important role in public policy discussions that regard it as an essential anti-corruption tool. This space is growing as new digital applications and solutions with potential in this field appear. Nevertheless, causal evidence on the impact of specific technological tools is still scarce. This evidence deficit is not unique to technological initiatives. In fact, because corruption is difficult to study quantitatively there is little knowledge about the impact of anti-corruption policies of any kind.

In recent years, quality studies on these issues have begun to appear. This chapter's objective is to document different technological tools' effectiveness in corruption control. Moreover, an effort is made to understand the reasons that explain why some innovations prosper and others do not. The latter is crucial to embark in a prospective analysis of the state-of-the-art tools that are starting to be applied in some contexts but that are yet to be evaluated because of their novelty. This review assesses the methodological rigor of the studies considered giving greater weight and priority to those that show causal relationships in a credible manner.



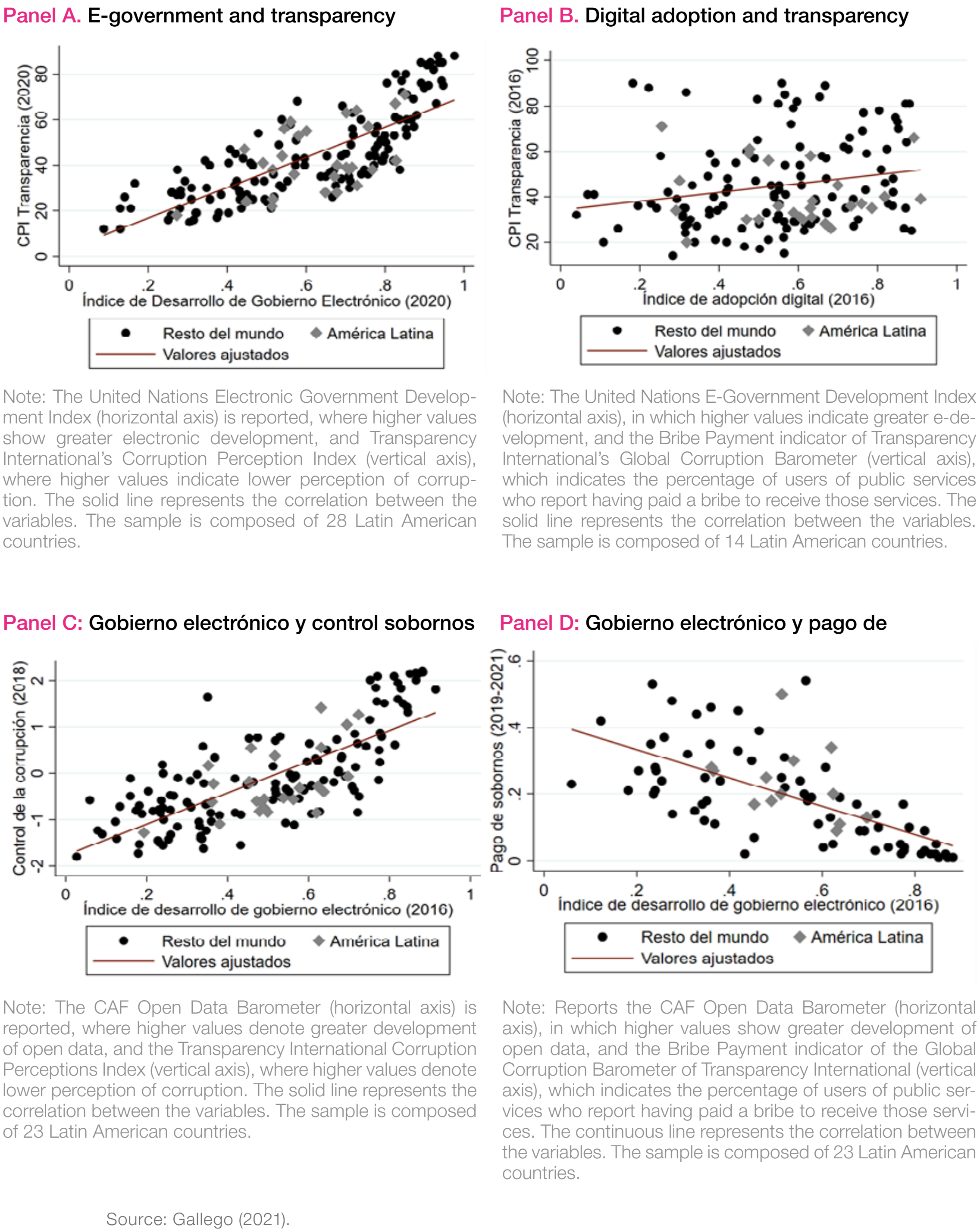
2.1.1. A closer look at the evidence on the link between digitalization and integrity

Before embarking on the causality analyses it is important to highlight that, according to multiple aggregate indicators, there is a clear correlation between the State's digitalization and corruption control (Gallego, 2021). For example, countries with higher values in the United Nations Electronic Government Development Index (EGDI) also show better results in Transparency International's Corruption Perception Index (CPI). As shown in Figure 2.1.

This correlation is robust to the use of alternative measures of digitalization or corruption. For example, in panel B of Figure 2.1, we replace the EGDI with the World Bank's Digital Adoption Index (DAI). In panels C and D, the CPI is replaced, respectively with; the World Bank's World Governance Indicators (WGI) corruption control measure; and, a self-report measure of bribe-paying from Transparency International. In all cases, the same relationship is maintained[24].

[24] In panel D, the sign of the correlation is negative because the corruption indicator used there takes higher values when corruption is high, contrary to the indicators in the other panels.

Figure 2.1: Correlation between digitalization and corruption in Latin American countries



Panel A. E-government and transparency

Note: The United Nations Electronic Government Development Index (horizontal axis) is reported, where higher values show greater electronic development, and Transparency International's Corruption Perception Index (vertical axis), where higher values indicate lower perception of corruption. The solid line represents the correlation between the variables. The sample is composed of 28 Latin American countries.

Panel B. Digital adoption and transparency

Note: The United Nations E-Government Development Index (horizontal axis), in which higher values indicate greater e-development, and the Bribe Payment indicator of Transparency International's Global Corruption Barometer (vertical axis), which indicates the percentage of users of public services who report having paid a bribe to receive those services. The solid line represents the correlation between the variables. The sample is composed of 14 Latin American countries.

Panel C: Gobierno electrónico y control sobornos

Note: The CAF Open Data Barometer (horizontal axis) is reported, where higher values denote greater development of open data, and the Transparency International Corruption Perceptions Index (vertical axis), where higher values denote lower perception of corruption. The solid line represents the correlation between the variables. The sample is composed of 23 Latin American countries.

Panel D: Gobierno electrónico y pago de

Note: Reports the CAF Open Data Barometer (horizontal axis), in which higher values show greater development of open data, and the Bribe Payment indicator of the Global Corruption Barometer of Transparency International (vertical axis), which indicates the percentage of users of public services who report having paid a bribe to receive those services. The continuous line represents the correlation between the variables. The sample is composed of 23 Latin American countries.

Source: Gallego (2021).

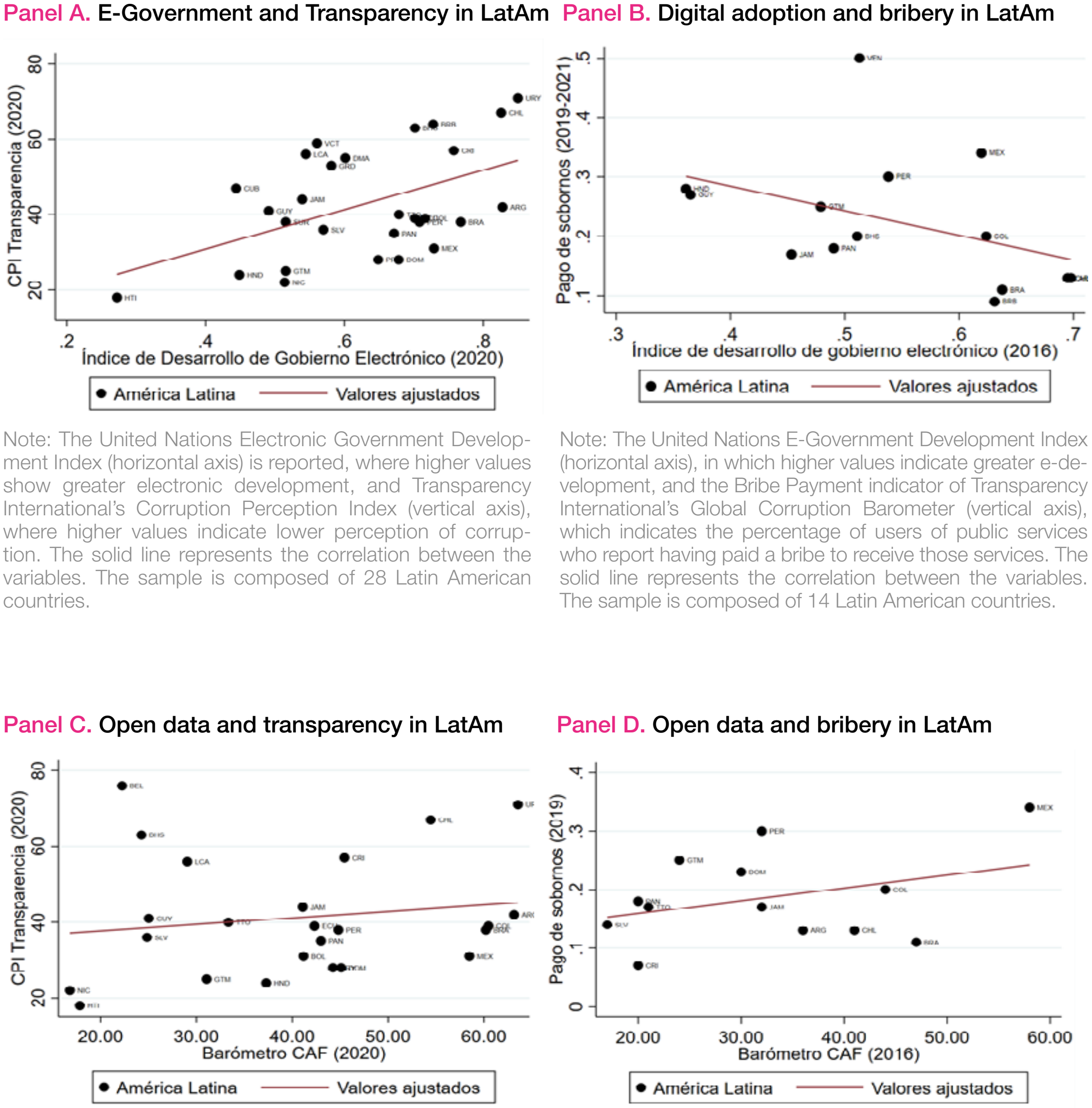
The general pattern holds when the sample is restricted to Latin American countries. EGDI is associated with lower perceptions of corruption (according to Transparency International's CPI) and lower reported bribe payments (again, according to the measure gathered by TI), as can be seen in panels A and B of Figure 2.2.

However, the correlation weakens or disappears when the Open Data Barometer is used as a measure of State digitalization (Figure 2.2, panels C and D). When looking at Latin American countries as a whole, this indicator does not have a clear association with levels of corruption.

The Open Data Barometer focuses on measuring the degree of data openness, while the EGDI comprehensively captures the use of digital solutions and tools in public management. Therefore, one possible interpretation of the correlations seen so far is that data openness alone is not enough to reduce corruption, and that a deeper use of technology in State management is needed in order to generate change[25].

[25] In that direction, some studies suggest that, in digital government strategies, the transactional element (i.e., the ability to obtain services and complete transactions with the state) is the most important in moving citizens' perceptions of transparency. Lizardo (2018) finds that electronic access to formalities and the quality of telecommunications infrastructure are the e-government components that correlate most with perceptions of corruption, while Valle-Cruz, Sandoval, and Gil-García (2016) find that the quality and completeness of government bodies' websites and digital communication channels are associated with better opinions about their transparency by the population in Mexican municipalities. Although these results are suggestive, it is important to note that they do not refer to specific interventions, nor do they analyze effects on actual levels of corruption.

Figure 2.2: Correlation between digitalization and corruption



Panel A. E-Government and Transparency in LatAm

Note: The United Nations Electronic Government Development Index (horizontal axis) is reported, where higher values show greater electronic development, and Transparency International's Corruption Perception Index (vertical axis), where higher values indicate lower perception of corruption. The solid line represents the correlation between the variables. The sample is composed of 28 Latin American countries.

Panel B. Digital adoption and bribery in LatAm

Note: The United Nations E-Government Development Index (horizontal axis), in which higher values indicate greater e-development, and the Bribe Payment indicator of Transparency International's Global Corruption Barometer (vertical axis), which indicates the percentage of users of public services who report having paid a bribe to receive those services. The solid line represents the correlation between the variables. The sample is composed of 14 Latin American countries.

Panel C. Open data and transparency in LatAm

Note: The CAF Open Data Barometer (horizontal axis) is reported, where higher values denote greater development of open data, and the Transparency International Corruption Perceptions Index (vertical axis), where higher values denote lower perception of corruption. The solid line represents the correlation between the variables. The sample is composed of 23 Latin American countries.

Panel D. Open data and bribery in LatAm

Note: Reports the CAF Open Data Barometer (horizontal axis), where higher values show greater development of open data, and the Bribe Payment indicator from Transparency International's Global Corruption Barometer (vertical axis), which indicates the percentage of users of public services who report having paid a bribe to receive those services. The solid line represents the correlation between the variables. The sample is composed of 23 Latin American countries.

Source: Gallego (2021).

Although the observed correlations show interesting patterns, these are insufficient as conclusive evidence on the impact of digital tools on corruption. In order to address that question, the rest of this chapter analyzes studies that estimate the causal effects of specific interventions set in different contexts. We will structure the discussion by classifying interventions according to the State tasks that mainly affect public spending, such as expenditure and investment monitoring, internal control, public procurement management, control and follow-up of transfers, and customs management.

2.1.2. Investment and public spending

One of the main mechanisms through which State digitalization can help curb corruption is by generating and disseminating information. As a general principle, if the expenditures and investments made by public entities leave a digital trail, the information available for citizens and oversight bodies to monitor them increases. This idea is consistent with evidence from recent initiatives in Latin America.

Investment

In recent years, platforms to disseminate information related to public investment projects have become particularly popular in the region. For instance the platform **MapaInversiones, developed with the support of the Inter-American Development Bank (IADB)**, is based on the experiences of **MapaRegalías** in Colombia. Since 2012 this platform has used georeferencing to provide information about the progress of public investment projects financed with royalties. In Costa Rica a platform called **MapaInversiones** has been in use since 2018. MapaInversiones is a web portal that allows citizens to access georeferenced information, make inquiries about different public investment projects and check their progress.

Rossi, Vásquez and Cruz (2020) evaluated the impact of MapaInversiones in Costa Rica by using a constellation of 649 public investment projects, managed and executed by 57 agencies from various sectors. The projects varied in size (from the procurement of school furniture to the construction of water supply systems) and amounted to a total of approximately USD 13 billion. A randomized controlled experiment (RCT) was conducted on that constellation and 460 randomly selected projects were published in April 2018, while the remaining 189 projects were published a year later.

The experiment's results suggest effects that appear quickly. In the short term (three months after publication on the portal), published projects showed a higher degree of physical (13.5%) and financial (127.4%) progress than unpublished projects. In the medium term (one year after publication) the impacts attenuated: the differences in financial progress were reduced to a still high 57.4%, while differences in physical progress disappeared. These results suggest that the digital tool's implementation had positive effects on project management, particularly in the short term. However, the authors did not discuss the reasons why the effect is greater on financial progress than on physical progress.

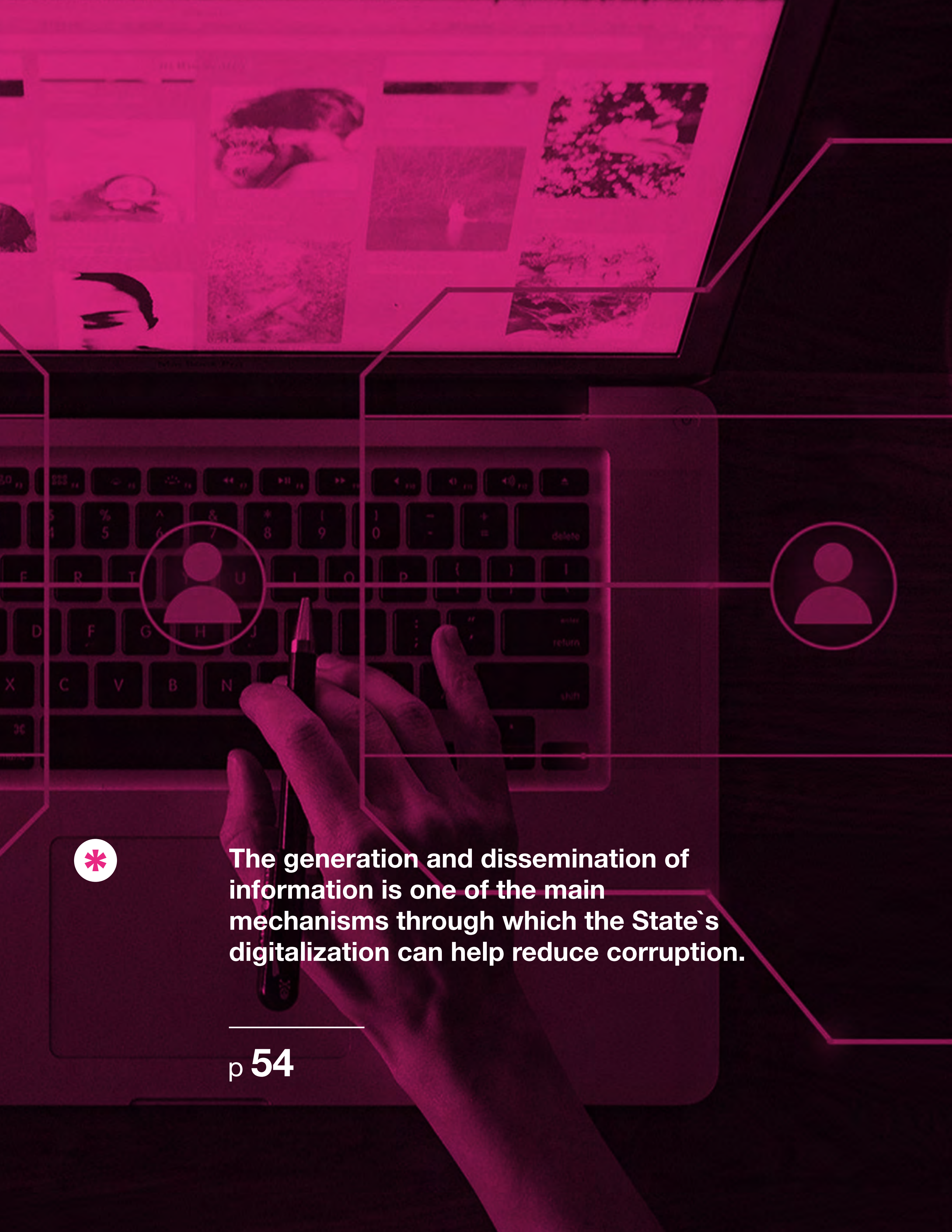
The platform also has functionalities that make it easy to share information through social networks or e-mails.

Two other interesting results emerged from the study. First, after investigating the mechanisms behind the observed impact, the authors pointed out that citizen's project monitoring increased as a result of the platform's implementation. Particularly, they show that the probability of a project receiving comments or observations increases by 7% when it is published on the platform. Second, they found that the effects occur almost exclusively in smaller projects, which is consistent with the idea that citizen monitoring may be more relevant for relatively simple and smaller-scale projects.

A similar case is the introduction of **MapaRegalías** in Colombia. This platform was launched in August 2014 by the National Planning Department (DNP by its acronym in Spanish) and presents georeferenced information and data on extractive sector royalties and the projects financed through them[26]. In MapaRegalías' web environment users can find project profiles that include information on the executed amount, its funding sources, the agency in charge, contractors and auditors, and a photo gallery to observe construction progress. At the department or municipality level data can also be viewed including the amount of royalties received by a jurisdiction, the projects financed by those resources, and the jurisdiction's hydrocarbon and mining production. The platform also has functions that make it easy to share information through social networks or emails.

MapaRegalías' implementation strategy does not allow the use of a rigorous methodology to clearly measure its causal impacts on project management. Nevertheless, Lauletta, Rossi, Cruz, and Arisi (2019) provide some descriptive data on the projects' progress rates before and after the site was activated. Based on a sample of 321 projects, the authors found that the level of projects physical progress increased by 7% on average after the introduction of MapaRegalías. Regarding the site's use, the authors noted that in 2016 (the last year observed in the study) it had 74 742 visits, showing a slightly increasing

[26] The development of this platform followed a more comprehensive reform of the distribution mechanism of resources from extractive activities, which materialized with the creation of the General Royalties System (SGR). The most important change of the SGR was the modification in the rule of distribution of resources, since royalties would no longer go mostly to the producing regions, but funds would be created to which producing and non-producing municipalities could have access, upon request. In addition, the monitoring, oversight and accountability mechanisms were also extensively modified. Gallego, Maldonado and Trujillo (2020) show that this reform had positive effects on the welfare of Colombian households by increasing the impact of royalties on the incidence of multidimensional poverty in the country.



The generation and dissemination of information is one of the main mechanisms through which the State`s digitalization can help reduce corruption.

p 54

trend since its launch[27]. Although data makes it possible to improve expenditure management it does not necessarily reduce corruption and the measured effects are generally linked and difficult to distinguish.

Public Expenditure

An experience that employs mobile phones is the intervention in the School Feeding Program (PAE, by its acronym in Spanish) in Colombia. Through PAE, the Ministry of Education transfers funds from the central government to finance meals in public schools. Its implementation involves the contracting and supervision of suppliers and is the responsibility of subnational governments (mainly departments and some certified municipalities). Following public complaints about food quality, the government decided to intervene in order to improve suppliers' compliance with contractual conditions. The intervention had two components: i) conducting continuous informal audits on food quality, and ii) sending weekly text messages to parents with information on the meals their children should receive in accordance with the providers' contractual obligations.

Keefer and Roseth (2021) found that the intervention had positive effects on operators' compliance with the contractually required menu. In terms of mechanisms, it is impossible to clearly separate the role played by audits and by the campaign to inform parents. However, the authors found clues that the latter had some effect. They particularly noted that text messages increased parental participation in PAE monitoring committees and meetings by approximately 50%.

The set of described cases shows that the use of digital tools to foster citizen control against corruption has produced mixed evidence. This is consistent with broader literature on the effectiveness of citizen monitoring to prevent and punish corruption, which has found widely varying results across experiences (contrast, for example, the work of Bjorkman and Svensson, 2009, and Olken, 2007). This apparent inconsistency reflects the fact that the effectiveness of this type of initiative depends on many contextual variables referring to; the details of the specific intervention under consideration; the type of corruption to be combated; and, the overall institutional framework's functioning.

In the case of transparency and open data policies, their value to generate change depends on whether the disseminated information complies with certain standards and whether it is used by control bodies and the public. Thus, the use of data by interested stakeholders reinforces the accountability process.

[27] In addition to facilitating citizen monitoring, MapaRegalías can facilitate official control within the State. By legislative mandate, executing agencies are required to upload project information to the platform (managed by the DNP) within a stipulated timeframe, with established sanctions in case of non-compliance. These well-defined responsibilities can facilitate the DNP's control task.

The Open Government Partnership proposes some standards in this area with the aim of controlling spending through digital tools in a more effective way. Unfortunately, there are no empirical studies that evaluate the impact that adopting this type of standards has on corruption. Nevertheless, there is descriptive evidence on the difficulties in adopting them. For example, Sheffer, Pizzigatti and Soares (2014) analyze transparency levels in Brazilian municipalities and conclude that their implementation has not fully complied with commonly accepted open government standards and technical requirements. The requirements that exhibit most non-compliance are those related to the structure and format of the data, the ease of searching and accessing them, and the possibility of automating the processes of extraction, processing and analysis (*machine readability*).

Similarly, by surveying citizens and officials, Cardona, Cortés and Wong (2015) found that the degree of transparency in Panamanian municipalities is low despite the implementation of government programs to promote fiscal data openness. For instance, 48% of municipal governments acknowledged that citizens do not have access to information on budget management. Moreover, when they do have access, it is generally through analog means.

Although there is regional interest in opening data and creating a culture of transparency enhanced by digitalization, these studies show that in practice there are still significant barriers for information. A direct consequence of this is the difficulty to exercise adequate citizen monitoring. Additionally, the gap between formal transparency policies and their effective implementation helps to explain the scarcity of credible evidence on these types of tools..

2.1.3. Internal oversight

In the previous section, we focused on tools that support citizen monitoring. Naturally, **technology can also be used to enhance the capabilities of government oversight bodies.** In particular, *machine learning* models can contribute greatly to the task of auditing accounts and transactions. The general idea is as follows: if you have a large database (with many variables and observations) of some type of official transaction (for example, public procurement of supplies) and information on which of these transactions presented irregularities, you can train a computing model to discover patterns associated with the incidence of irregularities in the observed variables. With that model, subsequent transactions can be evaluated to estimate their risk of irregularities. As more data is used to feed to the model, it will generate increasingly better predictions.

These are relatively new tools and, consequently, there is little evidence on their performance. The main obstacle to implement them is the need for sufficiently rich and systematic data to train functional models. Without data, these solutions cannot be applied. However, once the cost of this high input is overcome, these models can be a relatively inexpensive way to assess risks in public administration and to allocate human resources to audit and investigate them more efficiently.

Specific applications can be found in different areas. As suggested above, public procurement and contracting control is one of the tasks where these models have shown potential. Gallego, Rivero and Martinez (2021) discussed the usefulness of these approaches by training a model on data from two million public procurement contracts in Colombia in order to predict irregularities, contract non-compliance and implementation inefficiencies. Ash, Galletta and Giommoni (2020) explore another application for these approaches: the detection of corruption through government budgets. For this, they developed a model using detailed budgets of Brazilian municipalities and trained it with data on irregularities from official audits. The authors argued that the model's predictive capacity is high and that using its predictions to define where to audit would lead to an increase in the detection rate of irregularities, with respect to the current status quo in which audits are performed randomly. Finally, other authors have developed models to predict tax fraud, based on return and taxpayer data (De Roux, Pérez, Moreno, Villamil, & Figueroa, 2018; Solon, Rigitano, Carvalho, & Souza, 2016; Castellón & Velásquez, 2013).

Although there is no clear evidence on the effectiveness of machine learning tools, they seem like a promising way to improve internal control processes, particularly because they are a flexible instrument that can be progressively incorporated into traditional work protocols without generating costly disruptions.

2.1.4. Public procurement

Public institutions procurement of goods and services is a daily task. Given the resources involved and the room for discretion that exist, the risk of corruption in this area is a constant source of concern. In reality, there are no clear estimates of the incidence or magnitude of corruption in public procurement, but there is evidence that points to factors that increase the risk of irregularities in bidding processes.

In literature, the risk factor most commonly pointed out has to do with bidding and contracting modalities because closed and discretional processes present more irregularities than open ones. There are examples of this. For instance, in the context of PAE in Colombia, Corredor (2018) showed that direct contracting of suppliers led to the provision of lower quality food at a higher cost. Brugués, Brugués and Giambra (2018) found that in Ecuador, private firms that have connections with public officials have a higher probability of obtaining government contracts than those without, particularly in cases in which officials have discretion in the contract's allocation. Zamboni and Litschig (2018) show that in Brazil, high-discretionary modalities (direct purchases, invitational tenders, and bids among previously registered suppliers) restrict competition and double the probability of committing irregularities with respect to low-discretionary modalities (auctions that do not condition competitors' participation).

However, in terms of time and attentions, more open and transparent processes are traditionally costlier for organizations and procurement officials. Public procurement legislation recognizes this trade-off and tries to find a balance between agility and control procedures.

In this context, **technological tools emerge as a potentially transformative innovation that can be incorporated into public procurement systems with varying degrees of depth**. At a superficial level, it is possible to announce procurement processes in advance and disseminate information to interested parties through webpages. Similarly, electronic platforms can be used to record transactions after their completion, which could facilitate their internal monitoring (by public bodies) and external monitoring (by citizens, the media, etc.). Finally, at a more advanced stage of digitalization, several public administrations have started using transactional platforms for their procurement processes. This has served them to manage the entire process: calls for bids, communications with bidders, decisions, and even disbursements (although it is also common for more partial solutions to be implemented).

These tool's promise lies in the fact that when compared to traditional methods they lower the cost of conducting open and fair processes. This is because they allow information to be better disseminated among

stakeholders thus making collusion between officials and specific companies more difficult. Moreover, systematically recording performed actions increases the probability of detecting irregularities. As discussed in the previous section, if such recording is efficient and sufficiently widespread, **it opens the additional possibility of using that data to detect patterns within government transactions and create alarm systems based on machine learning models**.

These tool's promise lies in the fact that when compared to traditional methods they lower the cost of conducting open and fair processes. This is because they allow information to be better disseminated among stakeholders thus making collusion between officials and specific companies more difficult.

The best evidence on the impact of digitalizing public procurement comes from Lewis-Faupel, Neggers, Olken, and Pande (2016), who studied data from India and Indonesia, two countries exhibiting high corruption levels. For Indonesia, the evaluated tool is a semi-electronic procurement system. This platform allows companies to perform online tasks such as; expressing interest; downloading information and technical specifications; submitting prequalification materials; questions and complaints; but excludes the offer's final submission, which must be carried out by traditional means. The replaced system was one in which all stages of the bidding process were carried out through traditional means, and in which information on the contract and each bid was published on the Internet after the process resolution. In the case of India, evaluated cases were e-procurement systems introduced by nine states (provinces) as of 2000, which aim to replace the traditional manual processes.

The contracts included in the study were mainly for construction works, specifically for roads in the case of India. In Indonesia's case, consulting contracts were also examined. Construction works were generally awarded to the lowest bidder, conditioned on their compliance with administrative and technical requirements, while consulting contracts were usually awarded using formulas that combined price and technical scoring among prequalified bidders.

The results showed positive outcomes on some indicators, but not on others. Some variables unaffected by the e-procurement systems were; the number of received bids; the prices of the winning contracts; the final cost of the works (including overprices or addenda); and, the project's total duration until completion. There were also outcomes on other important aspects: the probability of the winning bid being from a location other than the work's site increased (particularly for consulting contracts) as did the probability for the winning bid to be from pre-existing firms (again for consultancies).

Perhaps the most significant effect has been the increase in the quality of works. This was observed in the case of India, where a central monitoring program audits the quality of a random set of roads. The electronic procurement system is associated with an increase of between 10% and 20% in completed works' quality scores. The authors found that the reason behind the improvements was that implementing e-procurement allowed the selection of better suppliers.

Although Lewis-Faupel *et al.* (2016) could not observe variables directly associated to corruption reduction, the estimates showed that these platforms increased procurement efficiency: the traditional (manual) system led to contracts of equal price, but lower quality. This way, it is possible to assert that procurement system's digitalization reduces corruption risks that exist in traditional paper-based processes which open room for officials to collude with suppliers.

For Latin America, the only study in this area has been conducted on the COMPR.AR platform in Argentina (De Michele and Pierri, 2020). Some descriptive indicators seem to point to positive results in terms of prices paid and processes duration. Unfortunately, obtaining clear estimates of the causal impact of the platform is impossible due to data limitations and program implementation details. This is a topic on which the production of regional evidence would be extremely valuable.

2.1.5. Social transfers

A type of corruption that generates concern in many contexts is the diversion of public funds destined for social programs. It is common for these resources to go through several bureaucratic instances where risks of diversion arise. In response to this, an important use of technological applications is to increase tracing of funds as they make their way to legitimate beneficiaries. Specific solutions with the same objective may take many different forms. In this area, India's regional governments have become a testing and learning site. Next there are three relevant Indian cases whose effects were documented in rigorous studies.

The first case deals with the introduction of biometric identification cards for disbursement authentication in the National Rural Employment Generation Scheme (NREGS) a large social program that guarantees 100 days of paid employment to every rural household[28] in India. The project took place in the state of Andhra Pradesh, and generated two simultaneous reforms. First, it changed the technology used by people to prove their identity when receiving payments by replacing traditional identity documents with smart cards containing biometric information (the ten fingerprints). These cards were created through voluntary enrollment campaigns and were linked to newly established bank accounts. The second change replaced the organization in charge of managing payments. Traditionally, this was handled by public officials from the postal service or local development agencies. How-

[28] In addition to NREGS disbursements, the same reform was applied to Social Security Pension System (SSP) payments. Although we focus on discussing the case of NREGS, the effects of the reform were very similar for SSP.

ever, the intervention replaced them with banks that were contracted by the regional government to manage the disbursements' last mile.

Before the reforms were enacted, the *status quo* was one in which the state level government transferred resources electronically through various subnational levels until cash reached the local units, generally through post offices. There, beneficiaries withdrew the payment directly or through an intermediary using traditional identity documents. Under the new system, the state government transfers funds electronically to the bank, and in turn the banks transfer the funds to subcontracted companies that manage disbursements. Beneficiaries now withdraw payment using their biometric identification card.

En el *statu quo* (antes de la reforma), el Gobierno estatal transfería electrónicamente los recursos, atravesando varios niveles subnacionales, hasta que el dinero en efectivo llegaba a las unidades más locales (generalmente, a través de oficinas postales). Allí, los beneficiarios retiraban el pago, directamente o por persona interpuesta, con documentos de identidad tradicionales. Bajo el nuevo sistema, el Gobierno estatal transfiere fondos electrónicos a los bancos, y estos a empresas subcontratadas para la gestión de los desembolsos. Los beneficiarios retiran el pago usando la tarjeta de identificación biométrica.

An important use of technological applications is to increase funds' traceability on their way to legitimate beneficiaries.

Muralidharan, Niehaus and Sukhtankar (2016) analyzed the reforms' effects and found positive results in the three evaluated areas: payment logistics, beneficiary access and corruption prevention. In terms of logistics, reductions of up to 20% were observed in the time spent by individuals to receive their payments. In terms of access, there was a 17% increase in the number of households working and receiving payments under the NREGS employment program. Significantly, the intervention decreased the diversion of funds: while the benefits received by households increased by 24%, the amount of funds transferred by the government did not change. In other words, the intervention ensured that a higher percentage of the funds ended up in the hands of beneficiaries, rather than being diverted out along the way. The authors estimate that the reduction in misallocated funds was slightly above 40%.

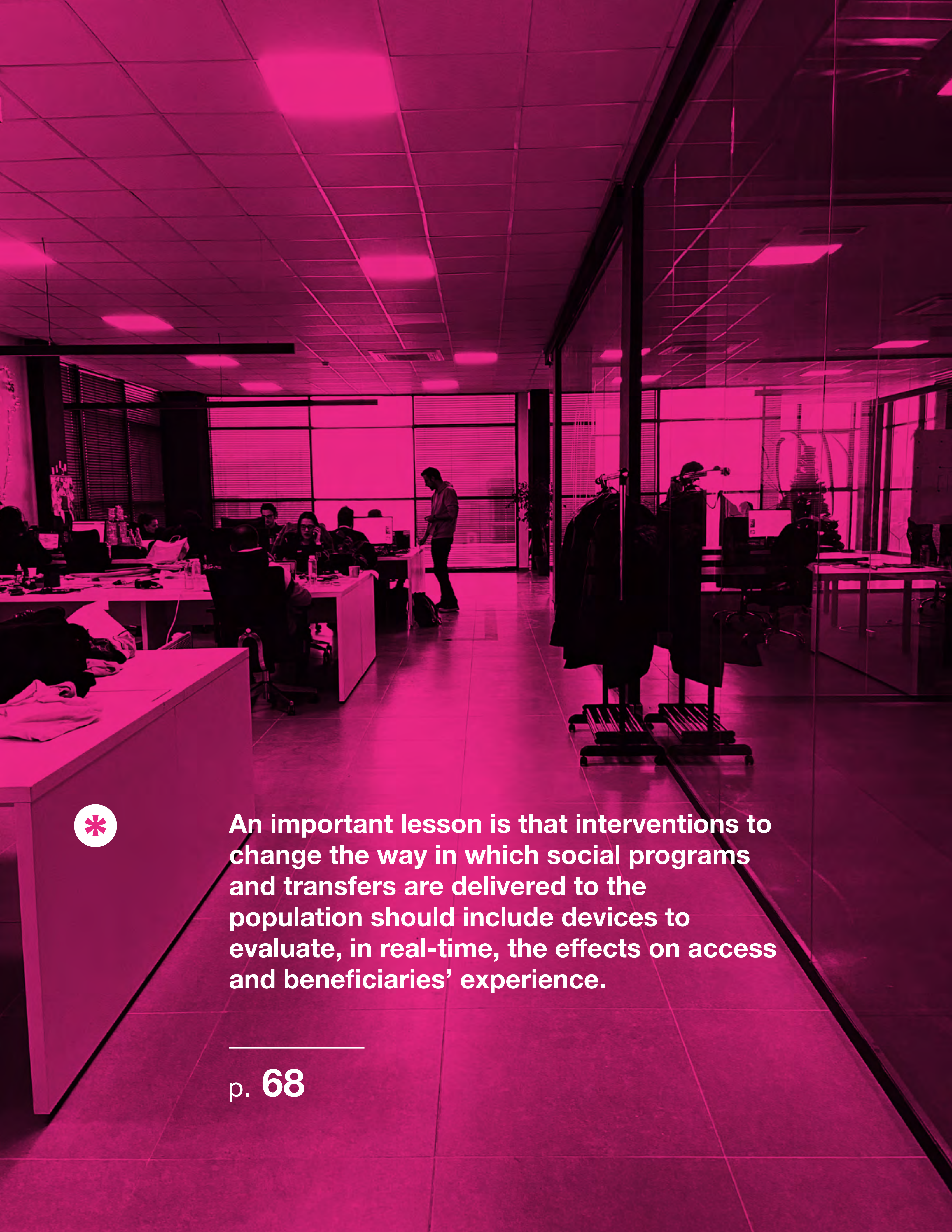
The authors embarked on an additional exercise to disentangle which aspects of the intervention produced the observed changes. Their results suggest that technological changes such as using the biometric information card to authenticate identity were responsible for the gains in access and for the reduction in funds diversion. Similarly, organizational change, namely the use of banks to manage payments, was responsible for improvements payment logistics and speed.

The second intervention case in India also involved the NREGS program, but was located in a different state, Bahir. In that case, the reform consisted of a mechanism to make transfers from the state government to the subnational levels "in real-time" rather than in advance. In the traditional system, when local government units in charge of disbursements to final beneficiaries ran out of program funds, they had to escalate requests for additional transfers. These requests were only accompanied by a “certificate of use” of funds, with no information on the identity of employed beneficiaries or payment amounts. The requests went up through several levels of government until they reached the state level, which then made the transfer. Eventually, local governments had to report information on specific beneficiaries and payments, but this typically occurred months after the payments had occurred. After the reform, transfers were only carried out after local government units directly uploaded information on beneficiaries and payments made, which they had to do continuously through a digital platform.

This program implemented three simultaneous changes. First, the transfers changed from cash advances to cover future disbursements, to (almost) real-time transfers according to the work performed by NREGS beneficiaries. Second, the intermediaries channeling requests between local units and the regional government were eliminated. Third, because they had to continuously record information about beneficiaries in the system (something that, in the rural context of the program, could be significant) a cost was generated for the local government agents.

Banerjee, Duflo, Imbert, Matthew and Pande (2020) showed the results. First, they found that the reform reduced NREGS expenditures by 24%. Using data from an independent household survey, they found that the intervention did not affect the number of beneficiaries, received payments, or constructed projects. This indicated that **the reduction in expenditures was the result of less resource diversion, and that there was no drop in people’s benefits**. The only negative aspect found was an increased delay in to beneficiaries in receiving payments. This work also produced evidence showing a reduction in the program’s number of “ghost households” that were credited with payments. The authors attribute the reduction in corruption to the increased ability to monitor program disbursements, due to the continuous recording of beneficiaries and transactions.

The third intervention experience was linking the biometric identification system with the Public Distribution System (PDS) in India, a program that allows beneficiaries to purchase fixed amounts of basic food at highly subsidized prices in specific government stores. The initiative had two stages: first was the introduction of electronic points of sale (POS) in the stores, that required beneficiaries to use their biometric card every time they made a purchase within the PDS stores. In the second stage (called “reconciliation”), the government adjusted down the amount of food distributed to each store by using information from electronic transactions to calculate inventory levels available in each store. This stage was used to reduce resource diversion (in this case, food).



An important lesson is that interventions to change the way in which social programs and transfers are delivered to the population should include devices to evaluate, in real-time, the effects on access and beneficiaries' experience.

p. 68

Muralidharan *et al.* (2020) presented interesting results from this experience. First, they estimated that before the program's implementation, diversion of resources was equivalent to 20% of the distributed food's value. Contrary to their assumption they observed a very low incidence of fictitious beneficiaries leading them to conclude that leakages occurred almost entirely at the intensive margin (falsely reporting food deliveries to real beneficiaries). The introduction of electronic POS (without reconciliation) made little difference: it did not affect government spending on food for the PDS, nor did it affect resource divestment. Even though, on average the benefits received by individuals did not change, there were some relevant distributional effects. In particular, the probability that in a given month a real beneficiary did not receive food at all increased by 2.4%. This effect was concentrated in households where at least one member was unable to authenticate his or her electronic ID, and was regressive because the problem was more common in poorer households. Another relevant effect of the program's first stage implementation was an increase in beneficiaries' transaction costs, for two reasons: i) the percentage of unsuccessful trips to the stores increased (possibly associated with failures in the electronic POS), and ii) the opportunity cost of time spent buying food increased because electronic identification required the beneficiary's presence, while in the previous scheme, households had the flexibility to send other members to the store. The authors estimate the increase in beneficiaries' transaction costs at 17%.

The initiative's second stage (reconciliation) did have impact on government spending, both on the PDS and on leakage. For the PDS, the reduction in food spending was between 20% and 35%. Most of that reduction (66% to 75%) was due to a drop in food disbursements. However, a non-negligible portion (between one-quarter and one-third) originated from a decrease in food received by actual beneficiaries. Several implementation factors may explain the drop in benefits received by households. For example, the government may have succeeded in adjusting food deliveries to stores (according to very precise inventory calculations), but not in avoiding divestment in the supposedly accumulated inventories, thus creating product shortages in the stores.

In general, the initiative's effects are mixed, and it is worth synthesizing them by separating the two stages of the program: i) the use of biometric identification alone did not generate benefits and, instead, resulted in the exclusion of a modest but relevant number of beneficiaries and in an increase in transaction costs for households, and ii) the reconciliation protocol achieved a significant drop in the diversion of resources but it also caused a decrease in the benefits received by legitimate beneficiaries.

The analyzed experiences demonstrate that technology can have important effects for the administration of programs and social transfers. The nature of those effects will depend on political decisions regarding what aspects to emphasize and on the implementation's details. The intervention's goal was to reduce the resources lost to corruption in the various programs. This was achieved, but there were important differences in terms of tail effects. For example, the introduction of biometric cards for NREGS disbursements highlighted beneficiary access as a priority, and there were improvements in that dimension but there was no overall effect on the program's fiscal burden. In contrast, the PDS intervention succeeded in lowering the program's cost but neglected the access aspects and ended up decreasing program coverage among legitimate beneficiaries. An important lesson is that interventions that aim to change the way in which a program is run can have a significant impact on its fiscal burden.

The systems used to deliver social programs and transfers to the population should include devices to evaluate the effects on beneficiaries' access and experience in real-time. **In this matter, different technologies can also be useful depending on their availability among the population**. An example, documented in literature, is the use of telephone calls to representative beneficiaries' samples in order to ensure that they receive benefits adequately (Muralidharan, Niehaus, Sukhtankar and Weaver, 2021).

2.1.6. Customs management

A relatively basic and potentially powerful form of State digitalization is the computerization of customs procedures. An example of this type of initiative is the XXI Century Program enacted in Colombia through the National Tax and Customs Directorate (DIAN, by its acronym in Spanish). The program was implemented sequentially in the country's customs offices between the years 2000 and 2005. Its main objective was to digitalize procedures to allow users to declare their imports electronically.

From its design, it included elements aimed at reducing opportunities for corruption, which went beyond the digitalization of customs declarations. It reduced agents' discretion to determine when to inspect a user's cargo or documents. Instead, it transferred that decision to the system itself in accordance to objective criteria based on the case's risk profile and any inconsistencies in their declarations. Furthermore, there was an increase in the traceability and transparency of each customs agent's decisions which reduces the risk of inspectors agreeing to fraudulent declarations. This would also prevent under-reporting of quantities and values of goods passing through customs. In addition to reducing corruption, the program was expected to increase these procedures' efficiency by reducing time, process errors and user uncertainty.

Laajaj, Eslava and Kinda (2020) evaluated several dimensions of the program's effects with generally positive results. First, the authors found a substantial reduction in corruption. The reform reduced uncertainty on the duration of customs transactions, which is associated to less discretion room for agents to speed up or delay processes. Moreover, the number of judicial cases filed for customs corruption by the Office of the Inspector General (PGN, by its Spanish acronym) decreased. Management also improved beyond the reduction of corrupt practices. For instance, there was a decrease in the discrepancy between taxes owed and paid. The authors argued that these discrepancies occur because companies underpay by exploiting communication deficiencies between banks and customs. Likewise, digitalization has improved communication and the ability to verify payments before releasing goods. In terms of expediting procedures, after the reform, the number of days required to process the entry of goods was reduced by 8%, while revenue collection increased. Significantly, all this led to an improvement in the importing companies' productivity, which increased their added value by 7% and their employment rates by 6%.

Two important conclusions of this study should be highlighted. First, that the program's positive effects were due to the fact that the technological intervention was well integrated with changes in the processes and use of information for procedure management's decision-making. This was responsible for reducing agent's discretionary misuse; redirecting efforts to streamline processes; and, tackling smuggling and other forms of fraud. Second, the authors estimate that the benefits in terms of collection and growth were several times greater than the costs of computerization (estimated at US$9 million). This suggests that the investment generated significant returns.

The program`s positive effects were due to the fact that the technological intervention was well integrated with changes in the processes and the use of information for procedure management's decision-making. This was responsible for reducing agent's discretionary misuse; redirecting efforts to streamline processes; and, tackling smuggling and other forms of fraud.

Today we face the appearance of even more modern technologies with potential applications for this field. Artificial intelligence is a tool that shows particular potential to optimize resources to fight fraud and corruption in customs matters —as it does for public procurement management. For instance, in Brazil project HARPIA was the result of a partnership between universities and the Department of Federal Revenue (RFB, by its Portuguese acronym). The project aims at detecting different types of customs fraud through artificial intelligence (Digiampetri, Trevisan, Meira, Jambiero, Ferreira and Kondo, 2008)[29].HARPIA uses *outlier* data models to identify suspicious customs operations. It also includes an information system of foreign products and exporters seeking to assist importers in registering and classifying their products and suppliers. Using Brazilian data, Paula, Ladeira, Carvalho and Marzagao (2017) trained unsupervised *deep learning* models to detect exporters at high risk of committing fraud and money laundering. Preliminarily, the model shows potentially high predictive power.

Currently there is no causal evidence on the effects of using artificial intelligence-based tools. As can be expected from the study on procedure

[29] HARPIA stands for Risk Analysis and Applied Artificial Intelligence in Portuguese.

computerization in Colombia, these techniques will be effective only to the extent that they are integrated with competent bodies' management and decision-making processes. A potential benefit is that they could refine risk calculations for customs operations and help better detect unsafe cases, thus resulting in a more efficient use of control resources.

Reviewed literature still shows limited statistical evidence on the effects of State digitalization on corruption. This can be explained by several reasons ranging from the relative novelty of some of the digital solutions under consideration to the inherent difficulty of studying corruption empirically. Consequently, it would be highly valuable to accompany State deployed digital interventions with rigorous studies to document their results and assess their impact.

La revisión de la literatura muestra que la evidencia estadística sobre los efectos de la digitalización del Estado sobre la corrupción es aún escasa. Hay varias razones para esto, desde la relativa novedad de algunas de las soluciones digitales en consideración hasta la dificultad inherente a estudiar la corrupción empíricamente. Una consecuencia es que resulta muy valioso que las intervenciones digitales desplegadas por los Estados se acompañen de estudios rigurosos que permitan documentar sus resultados y evaluar su impacto.

Alternatively, from a qualitative standpoint it is possible to further explore the ways in which some digital government initiatives generated integrity results based on the analysis of specific national experiences, their operating conditions and their public policy objectives. This will be addressed in the following section, which examines some specific cases in Latin America.

2.2. Comparative analysis of digital transformation initiatives to curb corruption in Latin America

The digital acceleration experienced by the world over the last two decades is transforming the way governments provide services. This was exacerbated by the COVID-19 health crisis, not only because of the need to reduce the number of face-to-face channels for interaction, but also because of the speed and efficiency enabled by technologies in public management processes. On the other hand, increasingly informed and connected citizens and businesses have growing expectations on the quality and convenience of public services and demand more inclusive and transparent decision-making.

As discussed above, digital technologies can improve public sector information disclosure and increase citizen participation (see chapter 1 and section 2.1). By implementing a more strategic use of public sector data and information, digital technologies can benefit policy formulation, service design and improve participation, accountability and transparency at all levels of government.

Governments increasingly offer online services. However, this has not often led to significant changes in their back office structures and processes (OECD, **2016**). New digital technologies like social media platforms, mobile and smart phones and current approaches to the use of technology (e.g., open government data and big data) offer increasingly collaborative ways of working within and across administrations, and better mechanisms for interacting with the public. This can help governments to be more efficient, effective, open, transparent and accountable to their constituents.

This new stage of digital technologies' maturity and the increase in their use by governments is marking a paradigm shift from e-government to digital government. According to the OECD's 2014 Recommendation of the Council on Digital Government Strategies, this will be defined as:

> the use of digital technologies, as an integral part of government modernization strategies, to create public value. It is based on a digital government ecosystem composed of government actors, non-governmental organizations, businesses, citizens' associations and individuals that sup-

ports the production of and access to data, services and content through interactions with government (OECD, 2014a).

The main result brought about by this change is that digital government is no longer just about digitalizing services and achieving operational efficiency. Instead, governments are adopting a completely new conception of ICTs as a mechanism for strengthening public governance while making government more open, effective, efficient and integrating citizen preferences into the design and delivery of public services. Digital government is about new ways of delivering public value and making government services and procedures digital by design.

In the last decade, Latin American countries have advanced in implementing digital transformation strategies at different speeds. Most countries in the region have digital agendas and digital transformation policies for the public sector, which have generated significant technological transformations and adapted their legal instruments to allow for digital governance and an increasingly open government[30]. **The interest of Latin American governments in advancing digitalization is materialized in different instruments that plan and even decree digital government goals**, as follows:

- México recently published its **National Digital Strategy 2021-2024**. It is based on two main pillars: (i) transforming the Public Federal Administration by using ICTs to improve and transparentize government services provided to citizens, and (ii) increasing Internet coverage throughout the country to combat the country's digital divide.

- Colombia defined its **Digital Government Policy** through **Decree 1008 of 2018**. Its aim is to make public entities more efficient to meet citizen`s needs and problems and in so doing allows them to be protagonists in the processes of change through the use and appropriation of digital technologies.

- Perú is implementing its **Digital Agenda**, supported by **Legislative Decree 1412 of 2018** which aims to achieve a digital transformation that makes it a more transparent, competitive and innovative country, and that makes social improvement viable. Its main strategies relate to digital inclusion, accessibility and active citizen participation.

[30] OECD. Open Government. Global context and the way forward (2016). The OECD defines open government as "a culture of governance based on innovative and sustainable public policies and practices, which are in turn based on principles of transparency, accountability and participation that promote democracy and inclusive growth." https://www.oecd.org/gov/Open-Government-Highlights-ESP.pdf

- Chile is working towards a **Digital Transformation of the State**, with three fundamental pillars: (i) a Modern State; (ii) an Innovative State, and (iii) a Sustainable and Efficient State. To this end, the **Law for the Digital Transformation of the State** was enacted in November 2019, and other documents that constitute the roadmap for the State's modernization were defined.

- Argentina enacted the **Digital Agenda 2030** through **Decree 996 of 2018**. It aims to coordinate government initiatives to take advantage of digital technologies in order to develop an efficient and effective citizen-oriented government through openness and transparency.

- Brasil presented the **Digital Government Strategy 2020-2022**, through **Decree 10.332 of 2020**, which involves the entire country. With that decree, it aims to move towards a fully digital government, in which data and technology support better quality public services and policies. It also encourages states and municipalities to expand the supply of digital services and definitively end the use of paper.

Along with **implementation of digital technologies**, in Latin America there is a clear intention to apply digital government trends in internal administrative systems and processes, such as electronic public procurement, open data portals and digital procedures. Some of these digitalization areas have potential in terms of public integrity.

Digitalization of government services contributes to reduce corruption risks through at least three mechanisms:

- First, digital technologies limit the discretion of public officials through automation and the use of digital tools that make the provision of public assistance and services more efficient by reducing contact between government agents and citizens.

- Second, government's digitalization helps to increase transparency and control. By guaranteeing access to information, particularly if it is in open data format, transparency and accountability are increased. This facilitates control over administrative actions by citizens and auditing bodies. In other words, the exponential growth of data available for consultation, exchange and analysis acts as a driver for integrity in public management.

- Third, digitalization offers new tools for social control and citizen empowerment. Citizens are empowered to demand good government performance and to take part in proposals to solve public problems. For example, through interactive mobile platforms and applications, it is possible to measure public program's user experience. This way it is feasible to ensure an improvement in the quality-of-service delivery and implement public policies based on the needs of end users.

Latin America's digital government policies are quite broad if one examines the regulations and roadmaps adopted by each country. However, we can highlight at least three areas of digital government that generated integrity dividends: citizen procedures, public procurement and promotion of social control.

2.2.1. Digitalization of procedures for public integrity

Relevance

Considering that **one in five Latin American citizens paid a bribe to access a service** (Transparency International, 2019), **it is clear that procedures open room to a considerable market for abuse** by public officials over millions of users. The seminal work of Roseth *et al.* (2018) defines **government transactions and red tape as a set of requirements, steps or actions through which users request or enter information from a public entity to obtain a right or to comply with an obligation**. The range of rights and obligations that give rise to procedures is broad: from the most basic and common, such as obtaining an identity, to the most idiosyncratic, such as a judicial interdiction. In each Latin American country, between 1,000 and 5,000 procedures are registered within government services' portfolios. On average, each citizen carries out five procedures per year, and 89% —at least before the pandemic— were done in person (Roseth *et al.*, 2018).

As the use of digital technologies deepens, it closes room for corruption and abuse in citizen procedures. This is because digitalization makes procedures impersonal and uniform for all users due to its use of programmed algorithms. Such programming closes discretionary opportunities for officials who process citizen requests and makes them more accountable to other authorities because their actions are easily traceable through the data produced by administrative procedures that remains available for consultation (OCDE, 2003).

Use cases

Simplifying and digitalizing procedures related to identity systems are two essential elements for the development of countries and to fight

against corruption (World Bank, 2019). Face-to-face procedures for obtaining IDs are slow, vulnerable to corruption and exclude people with fewer resources (Roseth et al., **2018**). In an emblematic case documented by the IADB (Roseth et al., **2018, p. 18**), it took a senior citizen in Bolivia 11months to renew her ID. During the process she underwent several trips, and ended up agreeing to pay the bribe requested by a policeman in exchange for expediting the formalities.

Simplifying and digitalizing the process of obtaining and identity implies democratizing access to other rights and creating more egalitarian systems.

The **World Bank** (2021) estimated that in Latin America in 2018, approximately 34 million people (5% of the region's population) did not have a basic identification. Most of them belong to the poorest and most vulnerable groups. Consequently, the institution proposed the Identification for Development (**ID4D**) initiative and a guide aimed at creating secure and inclusive information systems (IS). Simplifying and digitalizing the process of obtaining an identity implies democratizing access to other rights and creating more egalitarian systems. This initiative has inspired some Latin American governments to digitalize and simplify the process to obtain an ID.

The implementation of easily accessible digital services through digital identification and authentication procedures can potentially curb corruption risks by limiting human interactions, and reducing processing times and spaces for discretionary decision-making by public officials (Roseth *et al.*, **2018**). Next, we address some examples from regional experiences on the matter.

Peru is moving on to a stage of digital modernization in public service and procedures simplification by implementing an electronic identification document (**DNIe**, by its Spanish acronym) or a digitalized application process to obtain the DNI or passport. However, the challenge faced by the country is to encourage the use of electronic documents, such as the DNI, or the use of digital procedures. Since national identity documents are necessary for all citizens, it is important for them to have access to the Internet or digital infrastructure. **This poses a challenge in the Peruvian case where only 40%** of households can connect to the Internet.

The state of **Nuevo León**, in Mexico, introduced digital authentication thus making way for digital services. In May 2020, it launched the platform **Acceso N.L.**, where it is possible to access an identity and pay taxes through simple procedures. The portal is new and there are still no analyses or evaluations available on its operation, processing capacity and reception among citizens. It is worth keeping this experience in mind because it is a sub-national government with an outstanding performance in terms of digital infrastructure and open government in Mexico (PDE, 2021).

Another subnational government that documented a positive experience by simplifying and digitalizing government transactions is the municipality of **Córdoba**, in Argentina, which has set up a channel for digital procedures through the platform Ciudadano Digital. Not only is the procedure for obtaining an identity digitalized, but the number of citizens who already have a digitalidentity has reached 727,608 out of a total population of 1.4 million (López-Azumendi, Facchina and Zapata, 2021). Córdoba expanded digitalization to other government transactions such as e.g.: (i) cadastral records for changes in real estate ownership and claims on real estate valuation; (ii) permits for land use and execution of private works, and (iii) business licenses applications. The process of simplification and digitalization in the municipality's departments, which cost about USD 1.5 million —at current prices, generated efficiency savings of about USD 3.7 million (López Azumendi *et al.*, 2021).

Streamlining and digitalizing transactions represents greater well-being for citizens while the government benefits from such simplification through savings in time and money. Brazil is an example of optimizing public resources through the digitalization of services and procedures on their federal government website, **Gov.br.** During the pandemic, the site reached the figure of **3,000 digitalized services** (approximately 70 % of the 4,300 services it offers) and expects to digitalize and redesign 100 % of government transactions by 2022. This allows citizens to perform and monitor their requests' progress and provides flexibility and security to users. Among the services that can be accessed are Emergency Assistance and the **Digital Proof of Life of the National Social Security Institute** (INSS by its Portuguese acronym). With these initiatives, the government claims to save approximately **USD 350 million** per year three quarters of which are savings for users.

Mexico City's (CDMX) **Digital Agency for Public Innovation** (ADIP, by its Spanish acronym) has acted along similar lines by designing a single digital platform system to serve citizens and reduce costs associated to micro corruption and interactions between citizens and public officials. According to **Claudia Sheinbaum**, head of Mexico City's Government since 2018, the digitalization of government functions finds its rationale in the eradication of corruption, sustainable and inclusive economic development and the improvement of government-citizen relations.

Despite the advantages offered by procedure digitalization, this modality still has a very low use in the region[31]. According to the study by Roseth et al. (2018) and CAF (2021), few government transactions can be completed online in the region. Even though, with the pandemic, the proportion of internet users able to access online services in Latin America exceeded 30% (Roseth, Reyes and Yee Amézaga, 2021). The low rates of digital use can be explained by several reasons that range from; the lack of basic preconditions for digitalization; to digital infrastructure differences in countries with large regional disparities; and, the preferences of citizens who find it difficult to navigate government digital platforms, or have more confidence in face-to-face traditional channels.

[31] According to figures from Roseth et al. (2018), the use of digital channels did not exceed 18% for various types of procedures on the continent

Remaining challenges

The initiatives outlined here are not primarily and explicitly intended to address corruption challenges. Still, there are many public integrity benefits associated with e-government to be expected (Santiso 2021; World Bank 2016; Dupuy and Serrat 2014; Zinnbauer 2012), such as the following:

- When coupled with adequate access to information for citizens, digitalized procedures allow them to easily exercise their rights and access government services without corruption interfering.
- Limiting bureaucratic discretion and automating specific processes to reduce physical interactions lead to a reduction in bribery opportunities. However, simplification must accompany digitalization processes because, if the paperwork remains cumbersome, it can open up an opportunity for intermediaries who often create a market for bribery.
- Digitalized procedures also increase transparency in transactions with public officials, as they make them auditable which discourages behaviors such as improper requests or unjustified delays.
- In some cases, administrations may receive feedback and evaluations from service users to monitor satisfaction and identify problems related to corruption.

The potential deployed by digitalizing procedures is not applied with the same speed in the integrity ecosystem and in the procedures of the public authorities charged with preventing, investigating and punishing corruption. We identified at least two opportunities for improvement:

- Channels to report corruption: Latin America has a poor record of organizing, simplifying and processing corruption reports in an expeditious and effective manner (CAF, 2019). Globally, digital reporting platforms that monitor the process of investigation and sanction in each reported case are practically nonexistent. In fact, these platforms only serve as repositories to publicize reported facts but not to expedite the restitution of citizens' violated rights (U4, 2016). These reports have not had the same treatment as the other procedures cited throughout this section. This may be because processing involves the concurrence of several authorities from the different branches of government.
- Procedures to investigate and sanction corruption: In Latin America, both judicial and administrative authorities concur in the investigation, detection and sanctioning of corruption cases. In countries such as Argentina, Brazil, Colombia, Chile and Peru, in addition to the judicial branch, corruption

> may be brought to the attention of control agencies or the public prosecutor's office. However, institutional arrangements such as these mean that each authority conducts its own processes, creating silos with their actions, and even use different information systems that hinder coordination and are likely to duplicate investigative efforts. This, coupled with the complex regulations for criminal, disciplinary or administrative prosecution of corruption cases, considerably limits the room that digitalization can offer in these government processes. Among others, some measures that could facilitate joint efforts by administrative and judicial bodies in the investigation and punishment of corruption are; digitalizing the information systems containing sanctions for corruption; implementing digital files; and, establishing or improving platforms to consult procedures and processes related to the investigation and punishment of corruption. Moreover, these measures would make the procedures for sanctioning corruption more efficient.

To meet these expectations, governments must simplify, streamline and make the processes and services related to investigating, detecting and sanctioning corruption more easily accessible. Digital transformations and administrative simplification strategies could be applied to procedures within the ecosystem that investigates and sanctions corruption. Such simplification and coordination are necessary for technological solutions to work and to improve the efficiency and effectiveness of judicial or administrative authorities thus enhancing their deterrence capacity.

2.2.2. Public procurement digitalization

Relevance

A significant part of public spending is allocated to procure goods, services and public works so public institutions can operate. This requires states to organize procurement and contracting systems, which including decisions on expenditures and investments. In turn, this involves defining government procurement processes and procedures, choosing supplier or contractor selection methods, the definition and criteria for such choices, and the way the contract will be managed, including, among others, payments and risk management (OAS, 2020). Approximately 30% of Latin American and Caribbean countries' national budgets is invested annually through public procurement and contracting.

At the end of the 20th century, *e-procurement*[32] systems such as on-line purchasing were developed. E-procurement is the combined electronic use of information and communications technology to manage procurement and supplies. This concept refers to the integration of digital technologies to replace or redesign processes (which are no longer managed on paper but in electronic files) for the procurement of goods, works and services (OCDE, 2015).

It was at the beginning of the 21st century that the use of e-procurement extended to public procurement and contracting. This facilitated the management of large volumes of spending activities regulated by complex public procurement laws. These reforms sought to; automate procurement processes; streamline and expedite them; and, to reduce the costs and time required. They also aimed to increase competition and concurrence among suppliers. Thus, e-procurement became a part of the expansion of e-government services.

The main objective for governments' adoption of *e-procurement* was associated to managing the procurement system's knowledge to support the decisions of public procurement agents.

The main objective for governments' adoption of e-procurement was associated to managing procurement system's knowledge to help support public procurement agents' decisions. Managing electronic files' information and using digital media for procurement allows; reusing data to better understand State entities' demands for goods, works and services; an improved understanding of the market and the options to meet public needs; better design of procurement strategies; and, the organization of a contract's execution to ensure its effectiveness (Cetina, Fonseca and Zuleta, 2021).

Implementation of *e-procurement* helps the integrity of public procurement processes through the following mechanisms (OECD, 2015):

- Free access to information related to public procurement through an internet portal for all interested parties (domestic and foreign suppliers, civil society, control bodies), such as:
  - relevant institutional frameworks, laws and regulations;
  - specific procurement processes for solicitation (e.g., procurement forecasts, market reference terms, calls for tenders or award announcements) and
  - the public procurement system' functioning (e.g., comparative price or supply conditions, monitoring results and other aspects publicly showing the results of the system).
- **Greater transparency in public resources' allocation** from the beginning of the budgeting process and throughout the public procurement

[32] Public procurement mechanisms underwent a major transformation in the late 20th century, inspired by the private sector. In the 1980s, firms began to use digital tools that transmitted standardized messages from computer to computer to improve efficiency in procurement processes by issuing shipping addresses, product identification and quantity, improving times and minimizing errors compared to mailing and telephone calls. In the 1990s, the development of ICT enabled ERP (enterprise resource planning) systems to facilitate the flow of purchasing processes, catalogs and purchase orders.

cycle. This allows civil society, the private sector and other stakeholders to know the authorities' priorities and their spending.

- **When public procurement portals are transactional, the windows for corruption are further closed.** For example, allowing online bids online for a contract reduces the possibility of collusion. By awarding contracts online and evaluating bidders, the opportunities for improper agreements to award contracts in exchange for bribes are also reduced.

- Permanent display of data and information on suppliers and signed contracts facilitates the action of authorities or citizens to exercise subsequent control over public official's actions.

Use cases

In **Colombia**, according to **statements** by the National Public Procurement Agency, Colombia Compra Eficiente (CCE, by its Spanish acronym) between 2018 and 2021 alone, the State generated savings of COP 946 280 million through the Colombian State Virtual Store (TVEC, by its Spanish acronym). However, despite the effort to digitalize public procurement and make contractual information available in open formats, there is still insufficient progress in terms of corruption prevention. The most important cases of anti-competitive and corrupt conduct detection come from complaints made after the awarding of contracts[33]. The issue of "multipurpose contractors" has also been documented (Enciso and Romero, 2020). These contractors took advantage of the COVID-19 health emergency to change or expand State's suppliers' corporate objectives to obtain directly adjudicated contracts.

The coronavirus crisis exposed risks and corruption scandals in emergency procurement. Several countries, including **Colombia**, **Chile**, Paraguay, **Perú**, and **México City**, proposed the release of emergency procurement information in open data platforms to facilitate fiscal control and citizen participation. Some of these countries have also implemented *dash-boards* where information on emergency procurement is available in real-time. Implementations such as these can be found in **Brazil** and **Chile**.

In 2020, all countries in the region and the world directed most of their resources to public procurement of hospital supplies and medicines to address the health crisis. Several countries in the region stand out for publishing data in open formats and the resulting transparency of their procurement. **Chile**, made **the open data platform ChileCompra** available to

[33] By way of example, it is worth mentioning Resolution 12156 of 2019 of the Superintendence of Industry and Commerce, by which three legal entities and two natural persons were sanctioned for having colluded in Price Framework Agreements processes, carried out by CCE for the provision of office supplies.

the public, there it publishes information on public procurement previously announced in their **MercadoPublico**. transactional portal. With this initiative, **the Chilean government guarantees the interoperability of its data among various entities**[34] **and encourages the development of new applications and reports based on data that facilitates its analysis, monitoring and fiscal oversight**. When compared with its original procurement budget in 2020, Chile had savings amounting to **USD 21 million** in the purchase of masks, gloves and alcohol gel needed to deal with the health crisis. Emergency procurement was just one of various sectors that generated savings that year.

With support from CAF, Mexico City has worked on its digital transformation through several axes. With the aim of promoting integrity and making more efficient use of technologies it implemented the Tianguis Digital platform (see chapter 3, box 3.1). According to **information provided there**, the use of technology in public procurement systems achieves: (i) lower costs associated with bureaucracy and goods and services acquired; (ii) reduced barriers for participation by increasing competition and disclosure of public procurement processes; (iii) streamline procedures; and (iv) reduce discretionary spaces in public procurement processes. Moreover, the data ensures interoperability between agencies, avoids work duplication and facilitates public management. Data captured in real-time makes it possible to identify corruption red flags in a timely manner allowing governments to act effectively and preventively to correct shortcomings. It is interesting to note that this platform is being developed as an open *source* tool[35].

Remaining challenges

Despite considerable progress in the digitalization of public procurement and contracting processes there are still areas for digital platforms to improve and ensure even more integrity in those processes, these include:

- **Extending the coverage of open data to the entire government procurement cycle.** Users can interact with public procurement systems since contract information is published digitally. However only parts of the data are structured and only at some stages of the contractual process. Consequently, transaction traceability is limited. Although it is not the gen-

[34] Chile. DatosAbiertos - ChileCompra. The data are oriented to an inter-institutional collaboration model, with the objective of enhancing not only the value of public procurement information, but also to offer a greater amount of data in defined formats, and complement them with existing data on the State. https:// datosabiertos.chilecompra.cl/Home/SobreDatosAbiertos.

[35] Open source is a software development model based on open collaboration, its benefits transcend ethical issues or the question of free software. These models lower the costs of software creation and implementation and broaden the participation of interested agents (in these cases, public entities, citizens, control bodies, multilateral organizations, etc.). In addition, the code has advantages in terms of updating and adaptation to specific contexts; for example, if a law were to be enacted requiring a change in some platform procedure, open source would allow for an immediate update, without relying on external software providers to evaluate the update request.

eral case in Latin America, countries like Chile, Colombia and Paraguay have advanced in implementing open procurement data standards.

- **Greater impetus to implement transactional public procurement systems**. "Transactionality" means that the processes of registering suppliers, selecting bids, awarding contracts and signing them must be done digitally. In other words, system users must interact and exchange information in real-time. The recorded information allows transaction traceability including user data, dates and platform activity. However, existing platforms are transactional only for some processes.

- **Improved interconnection of public procurement systems to generate reports that are compatible with other government information systems, particularly those of public finance and the integrity ecosystem**.

  - In Latin America, the centralization of State procurement processes by public procurement agencies incentivizes agencies to manage information according to standardized laws and regulations for each area of procurement. However, this is not aimed for compatibility with other information systems. In particular, tracing expenditure and evaluating fiscal performance and transparency in government budgeting process would be more accurate if all expenditure sources' information

systems (human resources, public debt, investment, procurement) were compatible in real-time (IMF, 2019).

- Additionally, public procurement information systems should be compatible with others in the integrity ecosystem. Corruption investigation and control authorities or agencies keep data on natural or legal persons sanctioned for misconduct in the award and execution of public contracts. However, **they do not necessarily maintain a real-time connection or verification on the actions of those sanctioned within public procurement's ecosystem. This generates risks because those criminally or administratively sanctioned could use corporate vehicles to continue contracting** with the State. An example of this recently occurred with a contract of the Colombian ICT Ministry worth USD 260 million.

2.2.3. The role of Civic Tech in the fight against corruption

Relevance

The relationship between citizens and governments can be framed within the "principal-agent problem" (Varian, 1992). In it the former entrusts the latter with the administration and management of essential public goods and services. Since not all the agent's actions (in this case, the government) can be observed by the principal (in this case, the citizens), this relationship presents information asymmetries. Applying proactive transparency standards reduce these asymmetries. However, making open data and public information available does not completely solve the principal-agent problem.

Therefore, it is necessary to activate other mechanisms for citizen participation in order to give more stakeholders a voice in the formulation and implementation of specific programs and policies. Therefore, control over the "agent" is both a function of the disclosed information and of the "principal's" (citizens) ability to exercise collective action to adjust the actions of the "agent" when necessary (Persson, Rothstein and Teorell, 2013). The Open Government Partnership argues that citizen participation is a natural part of public policy development. This is because those who are affected by government decisions have the right to be part of a decision-making process that recognizes and communicates the needs and interests of all participants.

With the aim of improving the provision of public services and influencing public policies, civil society organizations (CSOs) and governments are experimenting with digital platforms to encourage and project citizen's voices (Peixoto and Fox, 2016). Technological tools, particularly smartphones, serve to channel and organize citizen participation in government processes as part of a trend called **Civic Tech. This is defined as "any technology used by citizens to empower them or help the government to be more accessible, efficient and effective**" (Peixoto and Sifry, 2017).

When **governments articulate their digitalization policies with their accountability initiatives, they also activate Civic Tech or civil technology mechanisms.** An example described by the **OCDE** is Colombia's **Urna de Cristal**, which is administered by its ICT Ministry (MINTIC, by its Spanish acronym). This initiative aims to provide as many citizens as possible with the possibility to interact with the government, learn about project updates and participate by asking questions and offering proposals. Urna de Cristal has been used for macro and national advocacy issues, from consulting and informing citizens about the **Ten-Year Justice Plan**, to local anti-corruption issues in the school feeding program (Keefer and Roseth, 2021).

New digital technologies have the potential to enable and organize citizen control over the actions of public officials in the implementation of programs and policies or in the provision of public goods or services.

New digital technologies have the potential to enable and organize citizen control over the actions of public officials in the implementation of programs and policies or in the provision of public goods or services. There is still no systematic evidence on these digital innovations' effectiveness in reducing corruption. This is because these platform's success is measured by their reception among citizens and not by the institutional response to citizen participation convened by Civic Tech (Peixoto and Fox, 2016). This section describes some recent experiences from civic technology and digital government platforms that have been implemented in Latin America to enable citizen participation.

Use cases

Innovations in civic technology and citizen applications are being increasingly applied to fiscal transparency and participatory budgets. Because the objective of corruption is precisely to plunder public finances, public budget transparency is a fundamental aspect of integrity policies. Budget transparency implies disclosing all relevant information in a timely and systematic manner. It also requires certain standards of clarity, reliability, accessibility and usability of public data and reports on public finances. Multilateral initiatives such as the Global Initiative for Fiscal Transparency (**GIFT**) have promoted a data standard to implement budget openness in countries.

However, budget transparency can be more ambitious if it actively involves citizens from the moment governments define budgets and allocate resources for public investments. For instance, at the local level, participatory budgeting consists of calling on citizens to take part in the deliberation and decision of their city's budget allocation. This is also a more ambitious form of budget transparency that goes beyond open data.

In **Brazil**, enabling digital technologies to involve citizens in public budgeting became possible during the last decade. Peixoto and Sifry (2017) showed that the inclusion of remote voting (mediated by digital tools) to define and allocate the state-level budget in Rio Grande do Sul positively impacted participation rates, inclusiveness, and citizen involvement throughout theonline process. The authors show that participation rose by more than 12% (compared to the baseline of face-to-face participation), and that the profile of citizens who participated in the initiative was on average younger and more educated, although not necessarily more participatory. Nevertheless, there is still a lack of statistical evidence showing the impact that participatory digital platform budgeting would have on curbing corruption.

A combination of disruptive civic technologies was implemented in **Perú**, where the Ministry of Economy and Finance (MEF by its Spanish acronym) developed the **Investment Tracking System**, This tool links the Investment Bank's information with the Integrated Financial Administration System (SIAF-RP, by its Spanish acronym); the Electronic State Contracting System (SEACE, by its acronym in Spanish); and, other applications that allow investment tracking[36]. The platform was key in the **Virtual Operation** implemented by civil society organizations during the health emergency to follow-up with the economic reactivation program "Arranca Perú"[37]. Data interoperability between different public entities allows a more refined control of public spending than the one derived from an independent review of SEACE data. For example, the system is capable of gathering data from all the agencies involved in the economic reactivation program. Nevertheless, there is need to improve the accessibility of the databases and registration tools and to incentivize their better use by competent authorities.

New technologies are improving interactions between citizens and budget authorities. For example, in October 2019 **Paraguay** introduced a mobile application called **PresupuestApp** It serves to consult any public institution's approved budgets and expenditures and allows citizens to report irregularities directly to the Ministry of Finance (MHP, by its Spanish acronym). Experiences such as those of Brazil and Paraguay show that ICTs have considerable potential for collective action that allows citizen participation in their governments'

[36] Peru. Ministry of Economy and Finance. https://www.mef.gob.pe/es/?option=com_content&language=es-ES&Itemid=100828&view=article&catid=767&id=5903&lang=en-ES.

[37] Arranca Perú is a program that seeks to reactivate the country's economy in the midst of the health emergency caused by the coronavirus (COVID-19). It involves a series of investments in the country that will be applied to sectors such as transportation, housing and agriculture, among others, in order to generate jobs and mitigate unemployment due to the pandemic. The transportation sector alone will receive close to PEN 3.8 billion for the maintenance of the national and local road network; see Emergency Decree 070-2020 which establishes the road maintenance plan as part of the program: https://cdn.www.gob.pe/uploads/document/file/863907/DU070_2020.pdf.

actions and decisions. In particular, thanks to ICTs, the public can become a more active player in budget integrity policies.

New civic technologies also contribute to improve citizen reporting mechanisms. Countries with good performance in transparency indexes have whistleblower protection laws (OECD, 2016) that recognize the importance of encouraging citizens to report corruption-related crimes. In addition to laws, digital technologies can also be a resource to encourage and channel citizen reporting.

In Mexico City, the Digital Agency for Public Innovation (**ADIP** by its acronym in Spanish), through the **Citizen Contact Center**, joined forces with the city's local mayoralty offices to strengthen channels for citizen reports and complaints and to ensure that their requests are dealt with effectively. The aim is to expand the contact center through innovation and openness to increase citizen participation.

At the federal level, Mexico adopted the **National Digital Platform**, which was built collaboratively by citizens and local Anti-Corruption Systems, and is managed by the Executive Secretariat of the National Anti-Corruption System. The platform uses government data sharing to detect corrupt activities such as conflict of interest, collusion and improper procurement at the national level. Similarly, it allows citizens to easily identify datasets that meet their reuse and consultation interests to exercise social control and evaluates the data's quality and structure. If the data does not meet the necessary standards, then the entities responsible for the platform's information correct the reports and datasets. This ensures that citizens can reuse the information and exercise social control.

Remaining challenges

The approach outlined throughout this section shows how digital government can use data and digital technologies' potential to stimulate citizen participation and social control as forms of collective action in the fight against corruption. However, there is a major challenge in the monitoring and evaluation of digital platforms that enable Civic Tech's environment as a component of public integrity policies.

Much of the **research on digital participation platforms focuses mainly on citizen engagement rather than on institutional response.** The review of experiences is concentrated on aspects such as downloads, user numbers and interactions (for example, Gigler and Bailur, 2014). However, there is no clear evidence that interaction between government and citizens is a closed loop. For instance, it is unknown whether these platforms encourage the State to respond to citizen complaints, correct behaviors or solve problems. Consequently, it is also necessary to measure the level of institutional response[38].

The "principal-agent problem's" framework shows that citizens (*i. e.*, the principal) have more information about government actions and, in some cases, collaborate in those actions. However, there is no evidence on how such technologically enabled participation translates into concrete changes or responses in the behavior and integrity of governments (*i. e.*, the agent). In practice, existing literature seems to imply that platform acceptance necessarily leads to positive institutional responses. This could induce a. high degree of optimism, in both scientific literature and public policy practice, about the role of technologies in citizen participation (Peixoto and Fox, 2016).

Moreover, **relevant literature has not identified to what degree the space for citizen participation and control over corrupt agents is actually dissuasive** (CAF, 2019; Ryvkin, Serra and Tremewan, 2017). Ryvkin *et al.* (2017)

[38] This is also consistent with what is pointed out in the Lessons and Challenges in chapter 2, section 2.2.1. on citizen complaints and reports.

suggests the possibility that geolocation from corruption events reported in citizen participation platforms could have a deterrent effect. Literature on this matter still needs to identify the variables that could make Civic Tech's environment an effective tool for integrity. Digital government policies that implement platforms enabling Civic Tech's environment could strengthen their development and implementation through design improvements, such as:

- **Improving collection and use of data on citizens who use participation platforms both online and in-person.** These data and their results should be made more open, so that governments, CSOs and academia can reuse them to identify variables of interest and areas for improvement in citizen participation and control mechanisms.

- **Include mechanisms to measure and monitor institutional response to citizen petitions, complaints and reports into the design of policies for citizen participation, social control and accountability.** That follow-up should include objective aspects such as the number of requests effectively processed and closed and a subjective evaluation by users and CSOs of the quality of the institutional response received.

- On the matter of detecting and reporting corruption cases through Civic Tech platforms, **governments must keep registers and be held accountable for their open data processing until corruption cases and reports are closed**. This poses a challenge because it requires a collaborative environment between the different branches of government that allows them to share data on the investigation, prosecution and punishment of reported cases, when there is merit to do so.

- **Finally, citizen participation platforms must overcome the challenges imposed by social and regional disparities in Latin American countries in order to increase and encourage citizen participation and social control.** This implies increasing the connectivity and coverage of communications infrastructure, which on average still does not reach 60% of the population (Agudelo, 2021). Likewise, to facilitate citizen interaction these platforms must be designed with a differential approach. In general, reducing the digital divide is a necessary measure to enable the Civic Tech ecosystem.

2.3. Closing remarks and policy recommendations

Although challenges persist for the measurement of digital technologies' impact on reducing corruption, the review of literature and public policy experiences in government digitalization and the corresponding reduction of corruption risks indicate that **digital technologies are gaining importance as a fundamental component in public integrity policies. In this regard, it is important that new programs and policies** linking integrity and digital innovation have mechanisms to reuse data by applying experimental or semi-experimental designs that evaluate digitalization's effect in reducing corruption.

In any case, there are quality studies on some relevant experiences that provide productive lessons. In this chapter, the discussion managed to distinguish certain State functions subject to digitalization, such as::

- information dissemination for citizen control
- public spending transparency and auditing
- public procurement and contracting
- control of social transfers
- customs management
- citizen procedures
- citizen participation and complaints

Diverse digital solutions can be developed for each of these tasks. Although to a large extent the effects of each intervention depend on its design and implementation specificities, the compendium of experiences analyzed in this report reveals important impact patterns that can be expected.

Tools designed to promote citizen control show varied results among different contexts. This reveals at least two aspects. First, that implementation details have consequences. Second, that some types of corruption are more likely to be influenced by citizen control than others. Transparency can be particularly useful in small-scale forms of corruption in close proximity to the citizenry in which one piece of information is sufficient to infer irregularities. For example, knowing how many resources a school manages for specific procurements or projects may be enough for the affected communities to detect anomalies. In the face of complex forms of corruption, or corruption that occurs far from the last mile of service provision, it can be very difficult for citizens to discover something, even if they have access to pieces of information. This does not imply that the value of digital tools to disseminate information is questionable. Even if it does not have immediate effects against corruption transparency is a fundamental principle of government. Likewise, if these tools are to have a concrete impact on corruption prevention, they require constant evaluation and adjustment.

Very little is known about the effects of adopting open data standards in public management. For now, significant deficiencies in implementing these standards are well documented and generate large gaps between formal policies and real transparency. As a consequence of this difference, it is difficult to study this type of initiative empirically.

In relation to auditing tasks within the State itself, solutions based on *machine learning* seem promising.

In relation to auditing tasks within the State itself, solutions based on *machine learning* seem promising. Aunque no hay análisis disponibles de impacto, distintos estudios han entrenado modelos usando datos reales (de compras públicas, presupuestos municipales o declaraciones tributarias) que muestran buen desempeño predictivo y que, aparentemente, podrían usarse para dirigir mejor los recursos de auditoría y control que tiene el Estado. Una ventaja de estas herramientas es su flexibilidad para integrarse de manera progresiva a los métodos tradicionales de trabajo.

Electronic procurement and contracting platforms have shown an impact on some procurement performance variables (associated with the diversity and quality of suppliers selected) and not on others (associated with project costs and duration). Relevant literature is still too limited to be conclusive. Moreover, there is no rigorous study for Latin America. An encouraging aspect is that existing studies come from contexts with low institutional capacities (India and Indonesia) and, even in those contexts, there are visible positive effects. E-procurement platforms seem very valuable and their virtues will, hopefully, be enhanced as their use is systematized. This would allow increasingly richer and more complete recording of State transactions and open possibilities for additional data uses.

Using digital technologies to control transfers and social programs, has proved to be very powerful in reducing the loss of resources. However, these tools also create risks, particularly associated with the exclusion of legitimate beneficiaries from the programs in question. Each interventions' effects heavily depend on defined policy priorities and on implementation details. A general recommendation is that initiatives of this type should be accompanied by mechanisms to verify that access for legitimate beneficiaries is not impaired.

In the field of **customs management**, an experience in the computerization of procedures was reviewed which **evidenced a reduction in the incidence of corrupt practices.** It showed very positive effects on processes' speed, which in turn had an impact on the productivity and employment of importing companies.

The experiences reviewed also illustrate the mechanisms by which digitalization can have an impact on corruption. The clearest mechanism is the reduction of public officials' discretion to make certain decisions and record transactions. For example, in certain contexts, tasks such as registering social program beneficiaries or deciding which cargo to inspect at customs can be highly discretionary and opaque. Automation of these processes is generally valuable, especially when it is easy to establish clear and algorithmic criteria guiding the decisions to be made (i.e., when discretion has no intrinsic managerial value).

Although at present there is little supporting evidence, a second poten-

tially powerful mechanism is the improvement of internal State intelligence through data generation and reuse. Digitalization opens room to the possibility of learning more about one's own management, and this has valuable applications against corruption. The best illustrations of this are the machine learning models to more efficiently control State transactions and operations.

Transparency is a third mechanism by which digitalization can have an impact on corruption levels. As previously discussed, this channel may be more effective against some corruption types than others. Moreover, transparency initiatives' impact depends on the existence of complaint and accountability channels (electoral, administrative, judicial) that are able to convert information into action.

Technology is advancing rapidly and new tools with potential applications in public management are constantly appearing. Latin American governments are beginning to recognize these trends and are adopting policies that will help to improve public integrity's potential in the fields of procedures, access to information and public procurement, among others.

Given the speed of things, it is difficult to clearly anticipate these solution's impacts. Even so, the **accumulated experiences give reasons to be optimistic about the role of digitalization in corruption, prevention. They also warn about the enormous importance of rigorously evaluating implemented tools**, to both maximize their impact and to avoid undesired collateral effects.

3.

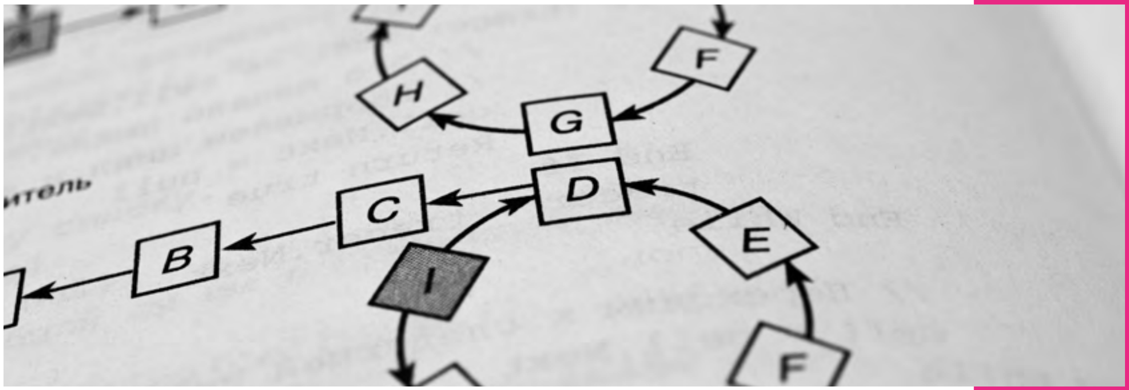
Data intelligence

“

I have checked it very thoroughly, said the computer, and that quite definitely is the answer. I think the problem, to be quite honest with you, is that you’ve never actually known what the question is.

Douglas Adams, The Hitchhiker’s Guide to the Galaxy

Data intelligence

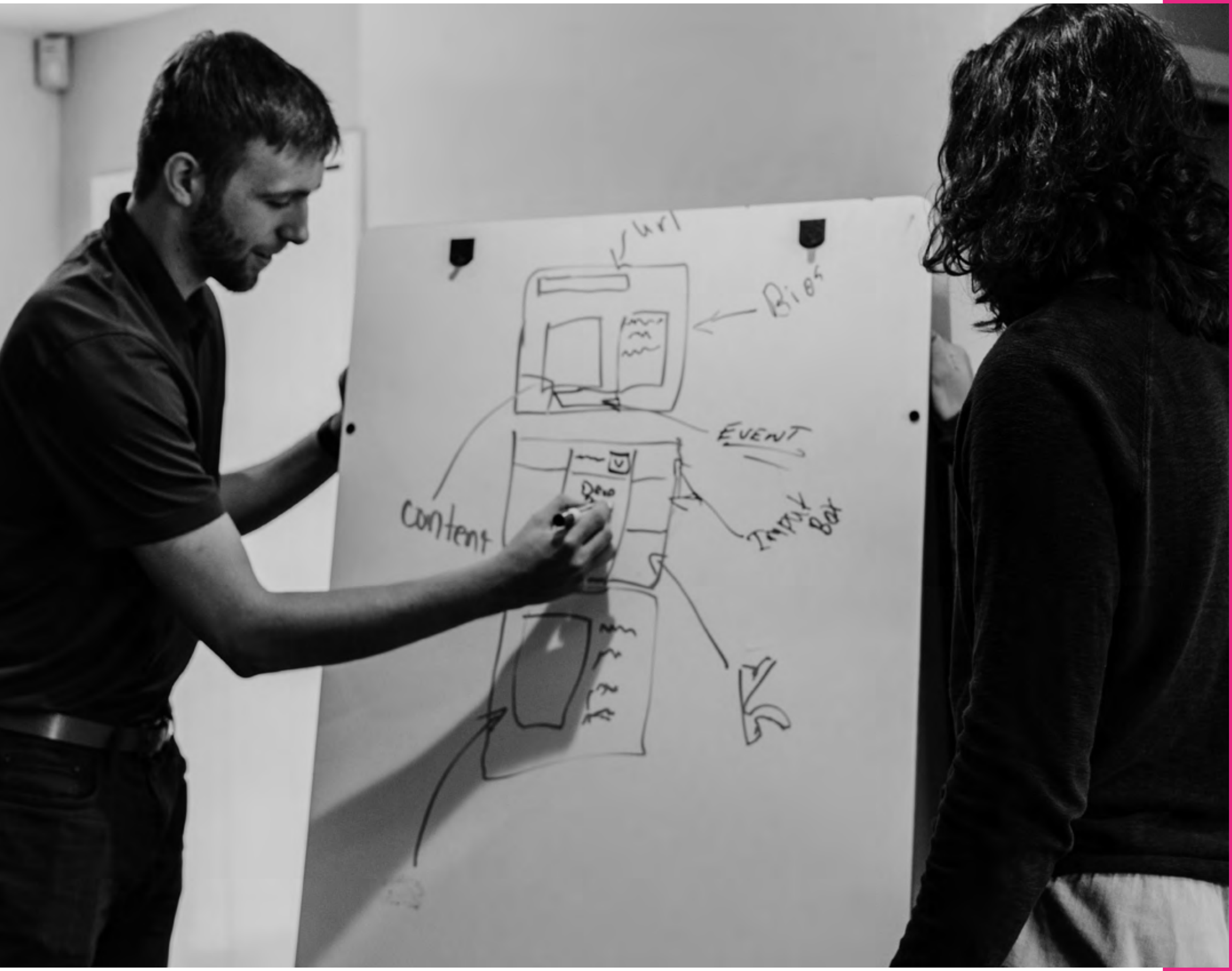


In Latin America, the first documented experiment that applied computational techniques based on decentralized data capture to government decision-making happened in Chile in 1970. The Synco or Cybersyn project was an initiative promoted by former President Salvador Allende and developed by the British consultant firm Stafford Beer. Cybersyn required a central computer connected to telex machines set in the factories so that data on production processes could be entered from location and then analyzed centrally. Information was consolidated in a hexagonal office, 10 meters in diameter, with room for seven swivel chairs and screens on the walls. Tables and paper were forbidden for analysts.

Cybersyn applied an early warning system by gathering data in real-time, designing statistical programs, building computer simulations of Chile`s economy and communicating with factories when problems affecting their performance were detected. The 1973 coup d'état would put an end to Cybersyn. Although that tool was intended for centralized production planning by replacing market institutions (which failed), its technology paved the way for what we know today as **"data intelligence"**.

Fifty years later, Cybersyn's seminal idea could not be more relevant to fight corruption in the region. Considering the digital acceleration that characterized recent years (see chapter 2), governments and multilateral entities are noticing the potential of tools that automatically capture information from processes and records governed by principles of proactive transparency and open data for application in areas such as public procurement and expenditure management, appointment of public officials and accountability of public entities. Unlike the prevailing order in Stafford Beer's time, currently technology to process abundant data has increased computing power.

When accompanied by an appropriate open data standard, new digital technologies' developments, modify policies to achieve more effective anti-corruption tools. As shown in Chapters 1 and 2 of this report, governments that possess enabling conditions such as digitalized services, proactive transparency policies and an open data agenda can take advantage of opportunities offered by the digital transformation to strengthen public integrity.



3.1. DIGIntegrity: definition and illustration

International experiences show the benefits of using technologies that combine predictive analytics and Macrodata to strengthen transparency; and the preventive approach in the fight against corruption. For instance, the World Bank developed an Automated System, currently in proof of concept, to detect potential frauds in procurement processes which it financed (Grace, Rai, Redmiles and Ghani, 2016). The project used a machine learning model to determine the probability of fraud occurring based on complaints or reports on procurement processes. It employed a gradient boosting method[39] and was trained using data from previous investigations in which both substantiated and unfounded complaints were found. The algorithm was tested by comparing cases when the system predicted corruption versus irregularities that were actually observed, and achieved a 70 % success rate in detecting cases of fraud, corruption and collusion (Grace, *et al.*, 2016).

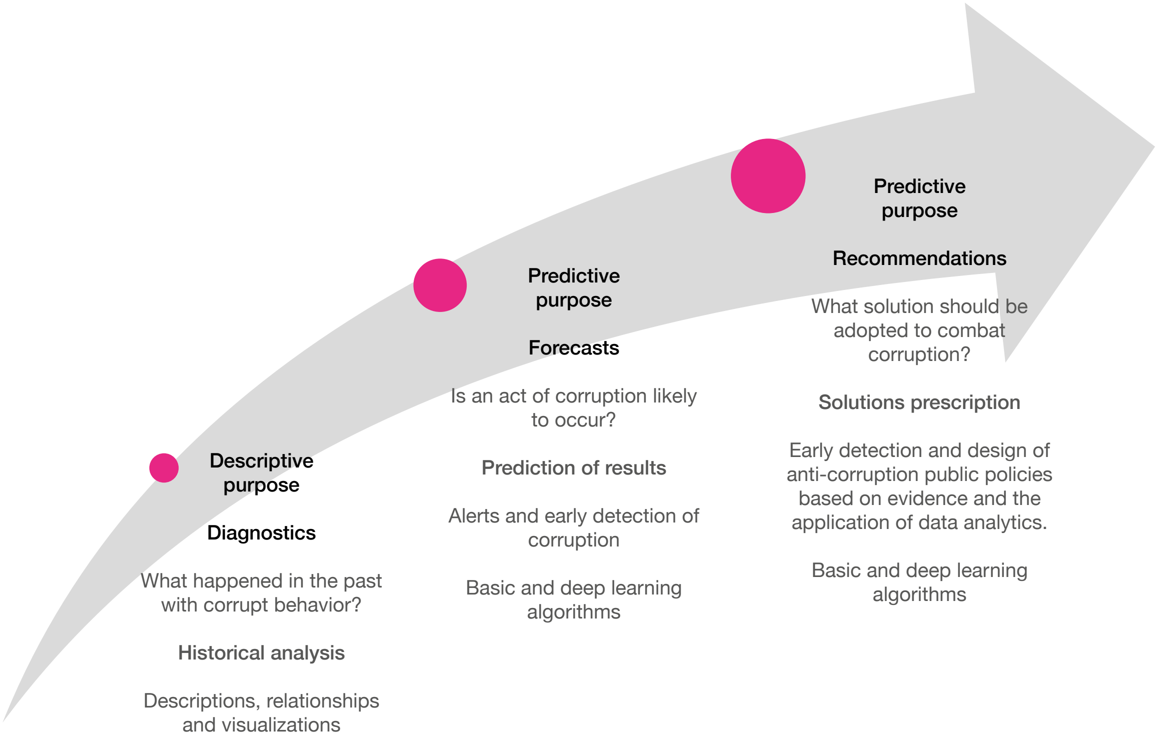
By combining predictive analytics and applying computing power for *macrodata* or big data processing, open data and data infrastructures open a window for taking large datasets and reusing them to prevent corruption.

Some governments are adopting a disruptive approach in their plans to mitigate corruption risks. This approach uses digital technologies and data processing to prevent, detect and investigate acts of corruption.

Some governments are adopting a disruptive approach in their plans to mitigate corruption risks. This approach uses digital technologies and data processing to prevent, detect and investigate acts of corruption. Although literature on the subject distinguishes four main uses: diagnostic, descriptive, predictive and prescriptive, these innovations specifically use data from descriptive and predictive models[40]. They also represent progress in the fight against corruption by allowing increasingly sophisticated analysis in the early and timely identification of corruption risks. The conclusions drawn from this information's analysis also serve to adjust public integrity policies based on evidence (see Figure 3.1). However, **for the scope of this report, we will group existing international experiences into two categories: descriptive and predictive models.**

[39] The model is produced from weak predictive prototypes, such as regressions, logit and probit models, and discontinuities, among others. Then, in a sequential and stepwise manner, they are combined to generate a more general predictive model (Rudin, 2012).
[40] See: https://www.oracle.com/business-analytics/data-analytics/

Figure 3.1. Evolution of the purpose of using data as an anti-corruption strategy


Descriptive purpose
Diagnostics
What happened in the past with corrupt behavior?
Historical analysis
Descriptions, relationships and visualizations
Predictive purpose
Forecasts
Is an act of corruption likely to occur?
Prediction of results
Alerts and early detection of corruption
Basic and deep learning algorithms
Predictive purpose
Recommendations
What solution should be adopted to combat corruption?
Solutions prescription
Early detection and design of anti-corruption public policies based on evidence and the application of data analytics.
Basic and deep learning algorithms

Source: Own elaboration.

Digital integrity initiatives, or DIGIntegrity, are based on data analysis. They employ two fundamental tools in different ways and to varying degrees: predictive analytics and macrodata (see figure 3.2). *Predictive analytics (PA) allows estimating or assigning a numerical value or probability score to the occurrence of particular types of corruption. To determine that probability —and create predictive models— it applies statistical analyses, queries and automatic learning algorithms to new and historical datasets (OECD, 2019; Waller and Fawcett, 2013).* ***Macrodata*** *(or big data)*[41] corresponds to large volumes of varied data that are processed at high speed in order to obtain information about strategic decisions related to the analyzed occurrences (Ortega, 2019). Macrodata analysts track specific patterns in the datasets by means of algorithms[42] that allow them to identify and assess pieces of information considered to be important for their individual auditing analysis or to determine corruptions risks.

[41] A dataset measuring more than a thousand terabytes can, at the time of this publication, be considered macrodata.

[42] An algorithm is a computational procedure (set of finite steps) that takes a value or set of values as input, and produces a value or set of values as output (Cormen et al., 2001). It makes it possible to analyze huge amounts of data and to select one option from an infinite number of possible decisions.

Figure 3.2.

Predictive analytics mechanism

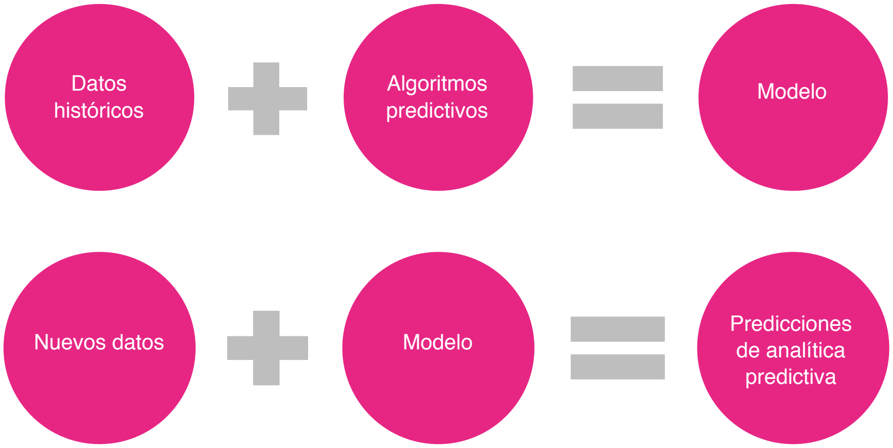


Figure 2.1. Source: Cetina (2020a).

Although its most common application is process automation, Artificial intelligence (AI) emerges as a tool that generates analytical predictions derived by processing large datasets. There are several definitions of IA, but all of them share at least two common elements: first, they imply developing computer systems capable of performing tasks that would normally require human intelligence;[43] second, they require large data amounts to train these systems to perform the tasks assigned to the AI. Computers capable of playing chess or go are part of the AI field, as are automated response or facial recognition platforms.

Data predictive analytics (PA) techniques can be based on basic and deep machine learning. *Basic machine learning* requires work to identify specific risks[44] or atypical behaviors at each stage of the procedure in which a higher level of transparency is sought. Once corruption risks are explicitly determined by experts and models are programmed to detect them, algorithms render their presence evident in the analyzed data and generate warning signals. *Deep machine learning* algorithms allow the analysis of both structured and unstructured data. Without previously defining corruption alerts or predictors, the software identifies patterns based on historical data from past corruption cases and generates models that are applicable to new data[45] (CAF, 2021). Thus, allowing the detection or prediction of possible corruption cases. This way, deep learning algorithms allow for data-driven decision making (Strusani and Houngbonon, 2019).

[43] Such as, for example, visual perception, speech recognition, decision making, cross-language translation and pattern detection, among others.
[44] For example, in the public procurement sector, there are lists of warning signs at each stage of the procurement chain (Volosin, 2015). Successive additions to contracts, long delays between the award of the contract and the start of its execution, or sudden changes in the corporate objects of the procurement companies, are some examples of risk in public procurement (Cetina, 2020a).
[45] Learning algorithms are automatically created from data, the richer the set, the better they perform (Strusani and Houngbonon, 2019), so that the programmed platform can make predictions decisions as a result.

This chapter presents technologies supported by data science that governments can implement in the area of public integrity and corruption control. Based on data usage's classification and evolution (see figure 3.1), this chapter presents case studies in which digital innovations employ data science as part of an anti-corruption strategy.

- **First, we analyze the technologies that allow the development of descriptive or diagnostic studies.** These aim at detecting corruption cases and strengthening public integrity by; reusing open data; expose relationships and constructing visualizations that help to identify and better understand corruption risks in public actions. These tools also allow control authorities and civil society to monitor and surveil public spending.

- **Second, we address predictive analysis technologies**. These methods allow to anticipate changes in the environment before they occur. To do so they assign, with high precision levels, a probability score for acts of corruption to occur. These technologies employ basic and deep learning algorithms (see figure 3.5).

3.2. Descriptive analytics

DIGIntegrity initiatives with descriptive purposes generally reuse open datasets to identify anomalies potentially associated to corruption risks (Cetina *et al.*, 2021). Free and direct access to information on government actions is possible by proactive transparency and open data policies combined with the use of digital tools to process datasets. This allows a comprehensive understanding of public management, and of corruption occurring within its environment.

Although it does not generate new information by itself, one of the most effective applications of technology and descriptive data analytics is visualization as it transforms the structure by which data is represented. Because humans have an easier time understanding information in graphical representations than in more complex structures (Few, 2014) visual tools such as this one permit processing large data volumes and presenting them in a clear and simple way. **The contribution of visualization does not lie in the data that feeds it, but in its ability to simplify data representation without losing information** (Chae and Olson, 2013).

3.2.1. Visual analytics for financial intelligence

Macrodata visualizations allow to detect relationships, patterns and anomalies in the data. These features guide and alert analysts to particular cases that require follow-up and further investigation. Visualizations permit identifying characteristics that would otherwise be difficult to detect through simple manual observation of databases. Known as *treemapping*, tools using mathematical techniques to translate multidimensional data (frequencies, moments, relationships or links), into intuitive figures (networks, nodes, clouds, heat maps and hierarchical schemes), are useful in detecting hidden relationships, demonstrating the existence of complex networks and tracing money flows.

The United Nations (UN) developed a platform to detect money laundering networks (goAML); and, a network exchange platform for financial intelligence information (goINTEL)[46]. Both are based on a relatively simple idea: to process

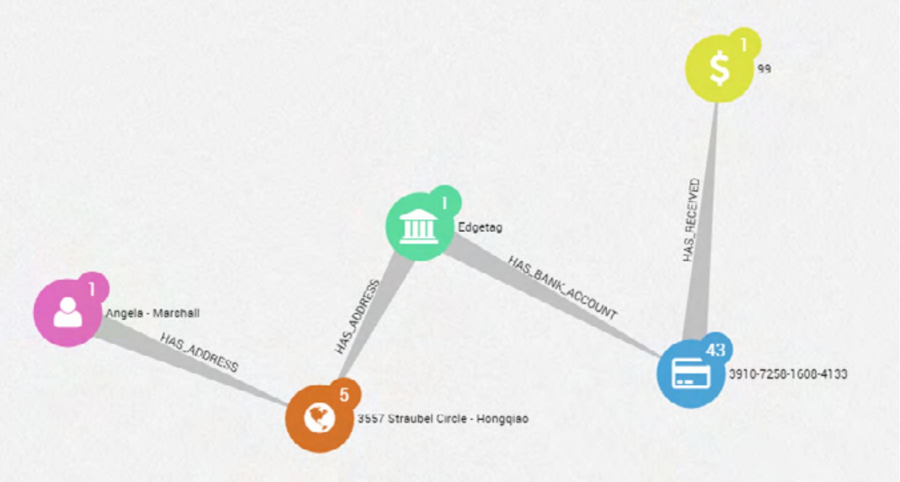
[46] This is part of an ambitious package called go Portfolio, which contains models and technological platforms to fight organized crime. According to the UN, some 125 countries currently use at least one of the applications contained in go Portfolio. See: https://unite.un.org/goportfolio/

large information volumes authorities can resort to analytical visualization of macrodata. Globally, over 49 countries have adopted goAML to detect money laundering and terrorist financing networks.

Generally, entities that provide financial services and others, such as, real estate intermediaries, report suspicious operations to financial intelligence authorities using Suspicious Transaction Reports (STRs)[47]. These are a fundamental input for financial intelligence task forces aimed at preventing and impeding the financial system's use to commit money laundering or to pay for bribes. Governments' Financial Intelligence Units (UIF, by its acronym in Spanish) process considerable volumes of information from STRs. The issue with recorded transactions is that they generate a data volume that cannot be analyzed using tabular methods[48]. As an example, consulting the United States' Financial Crimes Enforcement Network (**FinCEN**) portal on debit card money laundering activities in the United States yields over 37,000 results[49].

Figure 3.3.

Network of criminal transactions visualized from tabular data



Source: https://neo4j.com/blog/detect-investigate-financial-crime-patterns-linkurious/

GoAML displays techniques used in Latin America by governments' FIUs from countries such as Chile, Colombia and Peru, who have shared their experiences in recent years. The blueprint works in the following four phases:

[47] A STR (Suspicious Transaction Report) is made on transactions that, due to their amount and other characteristics, do not conform to normal business practices, of a given industry or sector, and are not reasonably justified. These reports are part of a Risk Management System for Money Laundering and Terrorist Financing (Sarlaft).

[48] That is, by examining functions and values in simple arrays of rows and columns, and then selecting data cells of interest.

[49] Note that we refer to only one possible crime, in one year, in one country, through one means of payment, and, in any case, a considerable volume of information is obtained. See: https://www.fincen.gov/reports/sar-stats.

1. **Data collection:** fund transactions are mapped. From there, the system suggests unusual transactions that must also be selected by the analyst. For example, instances where a group of people (natural or legal) use the same bank account, the same home address, have one or a few potentially fictitious suppliers and move large amounts of money within that network.

2. **Data analysis:** transactions are then re-filtered to determine which are in fact suspicious. Those are cross-checked with information concerning international transfers, cross-border financial asset exchange reports and others. Analysts then use the platform's information to refilter the transactions and highlight those that require investigation.

3. **Information Dissemination:** in this case, selected operations are reported to investigative agencies with judicial policing powers and to administrative authorities engaged in surveilling and regulating economic activities. There, the information is reevaluated.

4. **Interface development:** if a case is opened by the judicial police or investigative agencies then an interface is created for intelligence, investigative and judicial units to detect in real-time the movements of persons or corporations under investigation. This serves to confirm or rule out the existence of a network of illicit money flows.

3.2.2. Public investment visualization platforms

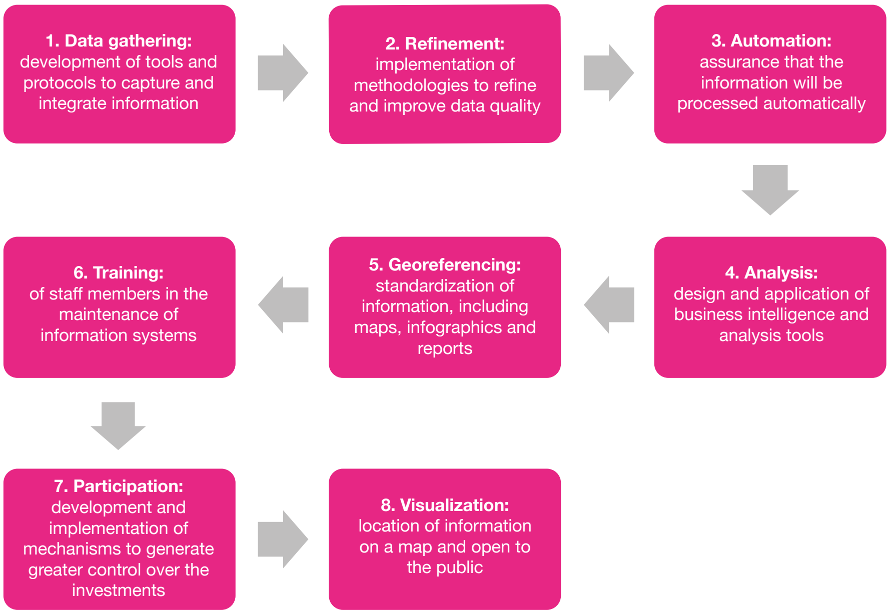
Public investment visualization platforms allow all stakeholders (citizens, private sector, civil society organizations and other State agencies) to monitor in real-time where and how public resources are invested. Data on public investments are collected, refined, automated, analyzed and geo-referenced in order to make them publicly available. Information visualizations are made accessible through an *online platform* with a unified and intuitive design that facilitates its consultation (see figure 3.4). When accessing information, interested parties can know, for instance; the number of public investment projects approved in a specific region; how many of them correspond to a given fiscal year; their progress status; amounts; and, the identity of contractors and auditors. This way, visualization eases monitoring and oversight of public spending by all interested parties.

Governments in the region are deploying geo-referenced and automated monitoring platforms to track public investments in order to improve their transparency and efficiency. An example of these platforms is **MapaInversiones** which was developed with support from the Inter-American Development Bank (IADB). The initiative was based on the experiences obtained in Colombia through MapaRegalías, a platform that since 2012, provides information on the progress of public investment projects financed with royalties. According to IADB estimates, MapaRegalías' module (see section 2.1) showed an average increase in the efficiency of projects physical execution approximating 8% (Lauletta *et al.*, 2019).

Through digital platforms, MapaInversiones provides users with access to georeferenced information and data on the progress of public projects in specific locations. (see section 2.1). These platforms allow information related to public investments in specific sectors to be immediately available and open to the public (see figure 3.4). Among others, examples of that information are those related to infrastructure investments, public utilities and health. Users can participate by commenting, contributing and uploading photos to verify the progress of specific projects (World Economic Forum, 2021). In order to transparentize spending and make it more efficient and effective, the public is made aware of the locations and manners in which government institutions invest public funds. Currently, Argentina, Colombia, Costa Rica, Jamaica, Paraguay, Perú and República Dominicana have MapaInversiones platforms providing information on how public resources are invested.

Figure 3.4.

Data processing in the MapaInversiones IADB initiative


1. Data gathering: development of tools and protocols to capture and integrate information
2. Refinement: implementation of methodologies to refine and improve data quality
3. Automation: assurance that the information will be processed automatically
4. Analysis: design and application of business intelligence and analysis tools
5. Georeferencing: standardization of information, including maps, infographics and reports
6. Training: of staff members in the maintenance of information systems
7. Participation: development and implementation of mechanisms to generate greater control over the investments
8. Visualization: location of information on a map and open to the public

Source: IADB, n. d.

In the context of COVID-19, special modules were created to monitor and transparentize resources allocated to address the health and social emergency (IADB,n. d.). Paraguay was the first country to implement the COVID-19 module, followed by Argentina, Costa Rica and the Dominican Republic. These modules' construction demonstrates that data and new technologies enable controls and transparency mechanisms in public procurement for emergency response by digitalizing processes that maximize the exposure of governments actions and allow tracking resource usage in real-time (Cetina, 2020b).

Control entities have also launched visualization portals for public works. To strengthen transparency in the execution of national works in Peru, the InfObras platform was created in 2012 by the Office of the Comptroller General of the Republic of Peru (CGR by its Spanish acronym) with support from the German Development Cooperation (GIZ). Within Infomapa, works can be tracked by; location; execution type; investment amount; start date; and, current status of the work. To date 106,265 works have been registered in the platform adding to a value of USD 71 million. In Chile, in 2014, the Comptroller General of the Republic (CGRC, by its acronym in Spanish) created the platform GEOCGR aimed at strengthening transparency and encouraging civil society participation. The portal provides geo-referenced information on the background of bids, opening of proposals, awarding, development of works, amounts and deadlines (Chile Compra, 2014).

Portals to visualize and monitor works exist at the national level and have also been developed by subnational governments. As of 2017, In Buenos Aires, the **BA Obras** platform allows interested parties to learn about the progress of public works under construction in the city. Using geo-referencing, the portal allows access to the details of a project's development by stages, communes and budget. Moreover, each project has specific information on the responsible government agency, its progress, contractor data, contract amounts and hiring process. The site has **open source software** allowing any municipality to replicate the website and **open data** for stakeholders to use according to their interest.

3.2.3. Network analytics in the fight against organized crime

Network analysis is a set of integrated techniques that represent relationships between actors to determine the extent and nature of the social structures that arise as a consequence of those relationships' recurrence. The basic assumption here is that the best explanations for social phenomena are obtained by analyzing the relationships between entities (Chiesi, 2001). This analysis is performed by gathering relational data that is organized as a matrix. If actors are represented as nodes and their relationships as lines between pairs of nodes then the social network concept becomes an operational and analytical tool that employs mathematical languages related to graph theory and matrix and relational algebra.

The techniques underlying network analysis allow researchers to specify indicators and control working hypotheses by defining and measuring traditionally general concepts such as social structure and cohesion. For instance, in the fight against corruption, the **Panamá Papers** case required **análisis de redes** techniques in order to expose the dimension of the illicit flows that were mobilized among thousands of nodes.

With support from CAF, Colombia's Office of the Inspector General (PGN, by its acronym in Spanish), developed an algorithm-based protocol to perform network analyses on corruption cases under its investigation[50]. As a starting point to develop this tool —and in the context of the Office of the Inspector General (ARCPGN, by its acronym in Spanish), data from the Mission Information System (SIM, by its acronym in Spanish) which compiles information pertaining to all disciplinary processes conducted by the PGN was comple-

[50] In Colombia, the Office of the Inspector General (PGN) is responsible for overseeing the conduct of public servants and private individuals who perform public functions or handle government resources.

mented[51] with existing public information from physical files. To that end, those files were digitized with OCR (*Optical Character Recognition*) algorithms so that, in turn NER algorithms (*Named-Entity Recognition*) could analyze them and extract the basic entities necessary to structure interactions.

The digitization of files with OCR and NER allowed to establish an Interaction Database (BdI, by its Spanish acronym). This serves to model corruption networks by identifying common nodes and interactions. These models allow extracting information on structures of macro corruption and institutional cooptation (Garay Salamanca, Salcedo-Albarán and Macías, 2018), informing about:

- The statistical frequency of natural and legal persons that are repeated in different cases.
- Certain natural and legal persons levels of influence.
- Nodes and agents that concentrate levels of direct centrality or intervention capacity.
- Interaction patterns and articulation of macro-networks.
- Number of networks and cases in which the same node/agent appears, among other levels of analysis.

Criminal Network Analysis can help identify illicit structures of institutional cooptation that do not operate on the basis of sporadic bribes but on that of systematic procedures occurring over long periods of time, and that are nonetheless susceptible to go undetected by investigation, prosecution and control agenciesl[52]. In Colombia, ARCPGN allowed developing models of highly complex and diverse illicit networks, in which thousands of nodes and agents establish thousands of interactions. In some cases, these networks can be referred to as “macro” because they are twice the size of a social network that can be directly apprehend and analyzed by the human mind (Salcedo-Albarán and Garay-Salamanca, 2016)[53]. A network of institutional macro-corruption and cooptation is one that is established to execute corruption schemes and that possesses a size that meets the complexity and characteristics of a criminal macro-network (Garay Salamanca, Salcedo-Albarán and Macías, 2018d).

[51] CAF found that the information recorded in some fields of the MIS had limitations of quantity and quality. The data were not structured and the way cases were described varied in level of explanation.

[52] However, the analysis, in itself, is not intended to serve as a support or input to ongoing research; rather, it is a support tool to identify hypotheses and courses of research.

[53] In general, the complexity of a network involving more than 300 nodes/agents makes it impossible, in practical terms, to memorize, associate and therefore understand the characteristics of the agents participating in such a network and their interactions.

ARCPGN analyzed three cases of corruption networks in Colombia that had national significance and with operations that could well have gone unnoticed:

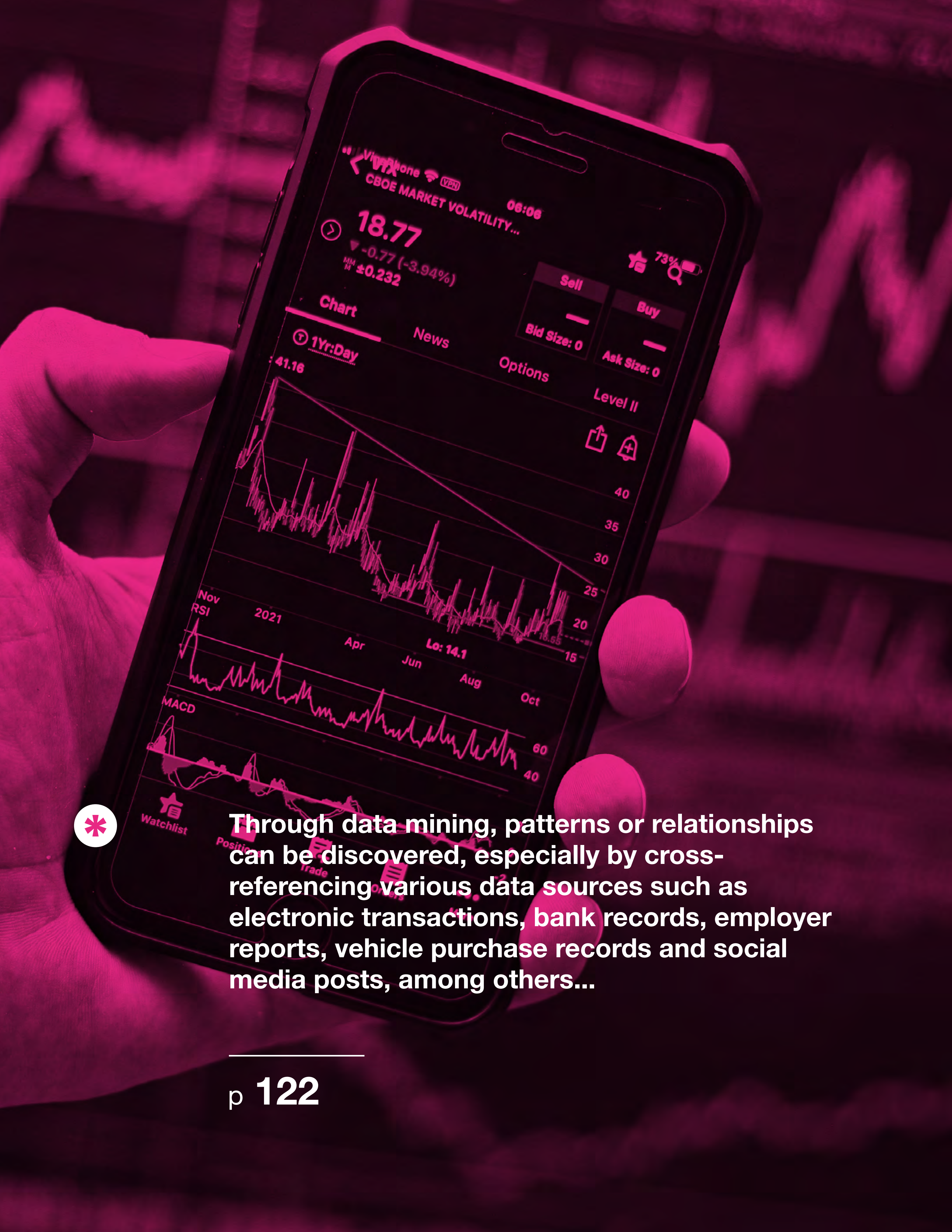
Criminal Network Analysis can help to identify illicit structures of institutional cooptation that does not operate on the basis of sporadic bribes but on that of systematic procedures over extended periods of time, but that are nonetheless susceptible to go unnoticed by regulatory agencies. investigation, prosecution and control.

- The **"health cartel"**, operated in the department of Cordoba diverting resources intended for medical treatment by creating fictitious patients and by taking advantage of the complicity of insurance companies and those providing health services to citizens. In this case, information from three files was consolidated in a unified Interaction Database that allowed to model a network made up of 287 nodes/agents related through 621 interactions. This contrasts with the PGN's information system visualization where only 21 nodes/agents and nine interactions were reported. This implies that the second model provides more information about the complexity of the analyzed phenomenon.

- The **School Feeding Program** (PAE, by its Spanish acronym) is the food supplement received by children in public schools and colleges in Colombia. With the complicity of procurement entities and interveners, exorbitant prices were charged for food and rations were sub standardized (Keefer and Roseth, 2021). After consolidating information from three files on deficiencies in implementing PAE in the departments of Guajira, Caquetá and Putumayo, the result was a network model constituted by 323 nodes/agents that established 555 interactions.

- The Odebrecht case, particularly the irregularities that occurred in the concession contract for the Ruta del Sol II highway. The firm Odebrecht paid bribes and financed political campaigns in exchange for the award of public works contracts (Garay Salamanca, Salcedo-Albarán and Macías, 2018d). After performing an analysis with ARCPGN a disciplinary ruling (complemented with judicial and administrative sentences), the PGN uncovered a network model of 162 nodes/agents with 266 interactions.

Network analyses identified illicit relationships and showed that some legal entities are constituted for the sole purpose of fraudulent procurement and incurring in actions that are penalized by criminal or administrative sanctions. Similarly, in the context of a structure of macro-corruption and institutional cooptation other corporate vehicles are established to commit apparently legal acts that in fact function to commit illicit objectives. Likewise, natural persons were detected who contract themselves through two different legal entities to capture resources from the State.



Through data mining, patterns or relationships can be discovered, especially by cross-referencing various data sources such as electronic transactions, bank records, employer reports, vehicle purchase records and social media posts, among others...

p 122

3.2.4. Publicizing public procurement for health emergencies

In order to ensure the necessary publicity and openness in public procurement (see Chapter 2) —even in the context of exceptional circumstances such as health emergencies— there are automated systems that allow data on public procurement in emergency contexts to be made public and open. These tools make data pertaining to, among others; the budget allocated to emergency response; government procurement; and, contracts available to all interested parties. This ensures that expenditures are made with the urgency and speed required during an emergency without sacrificing public procurement transparency.

An example of a technological solution to increase publicity and openness in public emergency procurement was developed in the United States. This solution is an automatic supplier alert system for government contracts. Registration is free and allows any company to be part of it. The platform matches an applicant's business type with on-going procurement processes using an automatic search system and then sends automatized alerts to interested parties by e-mail. This saves search time for potential bidders and maximizes publicity for government business opportunities. In this case, technology mediated by openness informs the market of urgent supply needs in real-time. This fosters an environment of control from both private sector and civil society so that an emergency declaration does not result in undue price manipulation or supply conditions.

3.3. Predictive analytics

Technologies that feed on open data and employ predictive analytic techniques allow generating corruption risk alarms or assessments in the early stages of government processes. By means of different data analysis techniques, these digital and information technologies advance the fight against corruption by allowing a shift from a reactive role to a preventive one. This is possible through data science (Llinás, 2003) because intelligent digital technologies have the capacity to estimate possible occurrences of corruption based on historical data.

Predictive analytics techniques can employ basic and deep machine learning[54] algorithms. Basic learning algorithms are used to analyze structured data. In these cases, a supervisor explicitly and previously identifies the risks of corruption or atypical behaviors at each stage of the procedure in which a higher level of transparency is sought. When the algorithms detect the presence of risks in the analyzed datasets a warning signal for collusion is generated. In the cases of deep learning algorithms, computers analyze structured and unstructured data such as images and text. Instead of being explicitly programmed, the software learns to identify corruption risks from data. An algorithm establishes the risks and communicates them to instances competent to perform control procedures while also exporting them to other databases for storage.

[54] Learning algorithms are trained with “training datasets” that are compared with the “validation datasets” to verify the construction of the algorithm. Then, “test datasets” are employed to measure the predictive power of the algorithm (Strusani, and Houngbonon, 2019).

Based on the findings of the individuals in charge, the tool refines its algorithm, forgetting the discarded cases and remembering verified corruption risks.

Figure 3.5.

Machine learning

	Basic automatic learning (*basic learning*)	Deep machine learning (*deep learning*)
Inputs	Structured data (tables in Excel format, CVS, tab)	Structured data Unstructured data (texts, images, videos, audios, e-mails)
Process	Supervised: an expert or supervisor establishes the rules or variables that will be used to analyze the data. The labeler knows the data behavior that it wants to predict, and the algorithm makes predictions by using the new data.	Unsupervised: the algorithm receives and explores unlabeled datasets and infers or discovers similar patterns or behaviors in them without having previously established rules or predictors.
Outputs	The software identifies the corruption pattern explicitly defined by the supervisor.	The software identifies corruption patterns according to the data's behavior without any specific predictors of corruption.

Source: CAF (2021).

3.3.1. Red-flagging

Risk system or *red flag* platforms use available information to establish risks and create patterns that predict an expected outcome in a given process. The flag is activated when the algorithm identifies the risk and a detailed analysis of the procedure that generated the alert ensues. A warning signal activating does not necessarily mean corruption exists but it does indicate the need for a detailed review of the case.

A data-driven innovation that addresses the preventive and monitoring approach in the contract awarding phase and to pricing by bidders comes from the **Korean Government's Collusion Indicator Analytical System** (BRIAS by its acronym in English[55]), which is administered by the Korean Fair-

[55] Bid Rigging Indicator Analysis System (BRIAS).

Trade Commission (KFTC). BRIAS uses open data generated by the country's public procurement system (KONEPS, by its English acronym) to build an automated system of risk indicators or red flags for potential procurement irregularities or inefficiencies. Within this system, data collection begins at the moment a user registers in the platform whether as a visitor, bidder or buyer. This way their credentials (IP address, dates and times of visit, modules visited, communications, etc.) can be used for statistical and analytical purposes.

The system calculates the probability of corruption in the selected bidding processes and may require additional information to further refine the algorithms.

The algorithms evaluate the following information:

- Number of bidders per bidding process
- Type and method for contractor selection
- Price of the winning bid
- Proposers' financial and organizational information

BRIAS collects the information from KONEPS, and performs a monthly automated data analytics process according to a minimum pre-budgetary threshold: bids above USD 423 800 and public works amounting to USD 4.2 million. In 2012, BRIAS detected 40 cases of collusion that led to fines of USD 847 million (OECD, 2016).

Another interesting predictive platform was developed in Hungary with the support of Transparency International (2015). This red flagging tool analyzes public procurement data and identifies corruption risks by emphasizing prevention and early warnings. Daily, algorithms analyze data from the *Tender Electronic Daily* (TED) to detect procurement processes with corruption risks

in accordance to 40 indicators built by experts. Once the threat is identified, additional information may be requested, and only cases presenting a “severe risk” are made public (European Commission, n. d.). Since its implementation until the end of 2020, the system generated early warnings for approximately 20,000 contracts.

Civil society organizations have also had important developments that facilitate citizen control over public spending. In Peru, the organizationOjo Público[56] developed an algorithm called FUNES[57], that searches for companies’ links that could help determine their success in a public bidding process. Since early 2018, Ojo Público has extracted information from public databases on contracts by the Peruvian State in order to investigate potential corruption risks posed by political and financial connections identified by FUNES[58]. This algorithm was written based on a development already tested by Mihály Fazekas from the Government Transparency Institute. That application is based on a system of red flags calculated by FUNES and based on categories such as; the level of competition among bids; their time of publication; their evaluation criteria; the time taken to evaluate proposals; awarded contracts; and, contractors’ contributions to political campaigns[59].

Ojo Público adapted the algorithm to the Peruvian context by prioritizing other indicators that identify possible corruption patterns such as, the potential links between a politician and the individual that will be potentially hired by the municipality or government. According to FUNES’ findings, “between 2015 and 2018, Peru adjudicated 110 thousand public contracts to a single bidder who had no competition and to companies created shortly before the bids occurred for the amount of S/ 57 billion (about USD 16.8 million)”[60]. This application works through a combination of text mining, network analysis and risk assessment to determine possible indicators for corruption in a public contract and then makes it available to the public.

[56] In allusion to the famous story by Argentine writer Jorge Luis Borges called Funes the Memorious, whose protagonist, after falling off his horse and suffering a head injury, can perceive things in detail and remembers everything. It was included in the book Ficciones (1944).

[57] Ojo Público is an investigative media outlet in Peru. In 2015, it received the Data Journalism Award for Best Investigative Journalism of the Year, granted by the Global Editors Network (GEN). In 2016, it won third prize in the Latin American Prize for Investigative Journalism, awarded by Ipys and Transparency International.

[58] See: https://ojo-publico.com/especiales/funes/

[59] More details in Fazekas and Kocsis (2020).

[60] https://knightcenter.utexas.edu/blog/00-21439-peruvian-investigative-site-ojo-publico-develops-algorithm-track- possible-acts-corrupt

Box 3.1.

Red-flagging.
Tianguis Digital Platform - Mexico City

Developed with support from CAF, Tianguis Digital, Mexico City's public procurement platform aims to improve the efficiency and transparency of the city's public procurement through three IT modules.

This technological development has three important phases:

Phase I: its objective is to facilitate digital management, competence and integrity in procurement processes through online clarification meetings and an algorithm that detects corruption risks.

Phase II: supports public monitoring and control at all stages of the procurement process through a digital contest and automated notifications to suppliers about procurement opportunities.

Phase III: busca fomentar la participación e inclusión en contrataciones públicas en la etapa de ofertas, mediante la implementación de un tablero de control interno y un visualizador público de contrataciones.

Using the **Open Procurement Data Standard - EDCA (OCDS)**, Tianguis identifies alerts in public procurement processes for instances such as: short bidding periods, low number of bidders in a process and high percentage of contracts with amendments. These alerts are displayed on the dashboard for process managers to verify and assess risks.

Source: own elaboration.

3.3.2. Combination of *big data* and visual analytics

Macrodata has enormous potential for government management and to strengthen tools in the fight against corruption. These large datasets can be used to construct basic learning algorithms and establish relationships to predict corruption risks or generate alerts. Once the risks are identified, intuitive visualizations are built networks/nodes, clouds, maps and diagrams, which guide and alert analysts to cases that warrant follow-up and investigation.

These large datasets can be used to construct basic learning algorithms that establish data relationships to predict corruption risks or generate alerts.

In Colombia, the Office of the Comptroller General of the Republic (CGR by its Spanish acronym), the entity charged with overseeing the proper use of public resources, developed a Contractual Information Central called OCÉANO. This platform gathers information from different sources including, but not restricted to; public procurement systems; the Information System for the Registration of Sanctions and Causes of Disqualifications (SIRI, by its Spanish acronym); the Identification and Civil Registry System; the National Tax and Customs Information System; and, the Single Business and Social Registry (RUES by its acronym in Spanish).

This digital tool establishes relationships between awarded contracts at the national level and examines them to detect possible corruption cases through a matrix analysis of networks and vectors construction. This has allowed the detection of irregularities in procurement which are prevented, controlled and sanctioned, as in the following cases:

- Detection of "procurement networks": nodes created by natural or legal persons that control State procurement in one or more regions and sectors without necessarily having the experience and suitability required to enter into such contracts.

- The use of business records belonging to deceased persons in order to contract with the State.

- The awarding of contracts to companies that have been sanctioned or that, having been sanctioned, use other corporate vehicles to cover themselves and contract again with the State.

- Public procurement indicators or concentration coefficients.

The platform, which operates within the framework of the recently created Directorate of Information Analysis and Immediate Reaction, has managed to analyze data from more than eight million awarded contracts between 2014 and 2020 which exceeded USD 250 billion in value. The CGR estimates that 27% of that procurement is assigned to repeat contractors, because they are either camouflaged in corporate vehicles, or because they constituted companies with dissimilar economic activities. The CGR reported cases in which the same person in a territorial entity is in charge of the acquisition of machinery, the provision of footwear, student refreshments and even the organization of pageants. In another reported case, the same company had contracts for markets, chicken purchasing, stringed instruments' maintenance, park installations and school meals. The data that feeds these instruments is obtained through 5,420 sources of information and through access to a network of 683 entities —including the National Infrastructure Agency (ANI, by its Spanish acronym), the National Planning Department (DNP, by its Spanish acronym) and the National Administrative Department of Statistics (DANE, by its Spanish acronym).

To arrive at these findings OCEANO builds sets of nodes or meshes. Using identifier data, the system is able to detect the contracting and procurement entities linked to the data, thus forming meshes or networks[61]. According to OCEANO's management, **the largest mesh** that has been discovered amounts to some USD 31 billion distributed among 208,000 contracts in a network consisting of 19,000 members. Analysis of this information allowed the CGR to report cases where contracts are allegedly awarded in an irregular manner.

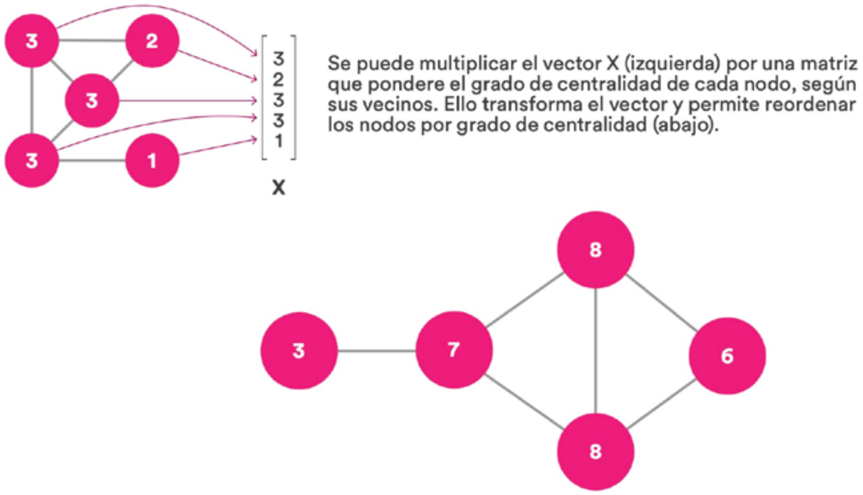
OCEANO's development is based on a combination of matrix network analysis and vector construction that predicts corruption risks in public procurement in real-time (see figure 3.5). Once the system is fed with both structured and refined data, each of them acts as a potential node that the platform analyzes by quantifying its repetitions (i.e., connections) in other contracts. Then an Eigenvector[62] is constructed by combining data on the number of links that a node has and the distance between nodes. This is used to program the system's algorithm and to construct a network or mesh of State contracts that expands the degree of intermediation of a node from the most direct (zero intermediaries) to the most mediated ones. By default, this construction will result

[61] These large datasets can be used for the construction of basic learning algorithms, through which relationships between data are established to predict risks or corruption alerts..

[62] An Eigenvector is the vector that, multiplied by a square matrix, yields the same vector multiplied by a scalar (the Eigenvalue). This has immense power in data science: if an Eigenvector is known for a linear transformation of data, one can calculate (predict) vectors for different data arrays that keep the same ratio (the same Eigenvalue). See Simon and Blume (1994).

in some outstanding nodes that are considered very frequent intermediaries by the algorithm, and will therefore be categorized as "high risk". This information is then visualized and constitutes the starting point for the CGR to generate early warnings for public procurement.

Figure 3.6. Criminal transaction networks visualized from tabular data



Se puede multiplicar el vector X (izquierda) por una matriz que pondere el grado de centralidad de cada nodo, según sus vecinos. Ello transforma el vector y permite reordenar los nodos por grado de centralidad (abajo).

Source: Cetina (2020a).

Enviar el texto de la traducción tipeado o la imagen ya traducida en en alta calidad.

In 2021, the Information Unit belonging to the CGR's Information, Analysis and Immediate Reaction Directorate (DIARI, by its acronym in Spanish) connected 7,411 sources of information corresponding to 878 connected entities in order to consolidate inputs for analytical models. During the same year, 758 risk alerts were issued amounting to USD 8,750 millon. For its part, the Immediate Reaction Unit showed the benefits of preventive and concomitant control processes that allowed safeguarding more than USD 375 millon in 28 completed projects and activating 169 projects amounting to an investment of around USD 1,850 million.

Digital tools currently used by DIARI establish relationships between contracts enacted nationally and evaluate them through a matrix analysis of networks and vector construction to detect possible corruption cases. This allowed the detection of irregularities in procurement that are prevented, controlled and sanctioned, as in the examples described below:

- Detection of "procurement networks": nodes where we can find natural or legal persons that control State procurement in one or more regions and sectors without necessarily having the experience and suitability required to enter into such contracts.

- The use of business records belonging to deceased persons in order to contract with the State.

- The awarding of contracts to companies that have been sanctioned or that, having been sanctioned, use other corporate vehicles to cover themselves and contract again with the State.

- Public procurement indicators or concentration coefficients.

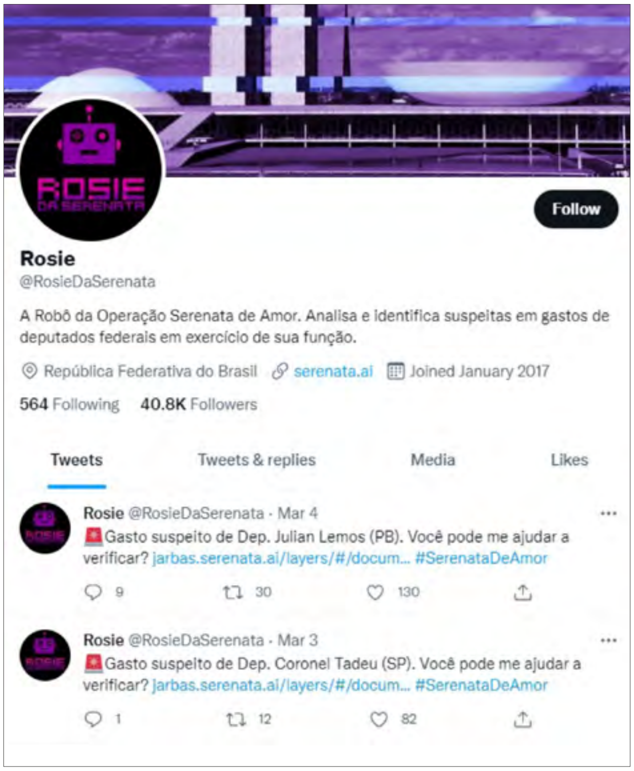
3.3.3. Artificial intelligence and social network analysis

By developing algorithms, artificial intelligence allows computers to analyze data, learn from it, detect patterns, and based on them, predict changes or events before they happen. This way, for instance, algorithms estimate the probability of corruption occurring based on a pre-identified set of risks within a given procedure. Once these risks are identified, automatic alerts are generated so all stakeholders can follow-up and corroborate or deny the risk's existence. This enables collaborative work to mitigate or report corruption risks, and allows greater social control and interaction between the private sector and citizens on public spending.

In Brazil, civil society organizations created an artificial intelligence robot that analyzes congresspeople's expense statements. Rosie is an open-source digital innovation that aims to empower civil society to demand transparency and accountability. As a result of a *crowdfunding* campaign, Operation Serenade of Love created Rosie in 2017, a robot that uses artificial intelligence to analyze data declared by parliamentarians and identify specific suspicious expenses. For example, payment vouchers indicating that a senator was in two different places on the same day and time (Cordova and Gonçalves, 2019). On a monthly basis, Congress receives more than 200,000 requests for reimbursements. Even though, these are largely processed manually, the copies of receipts used in reimbursement requests left records in open databases.

Rosie's creators studied the legal rules on disbursements and converted them into software code. Then they analyzed possible ways to circumvent the regulations and determined the kind of record that such an irregularity would leave on existing data. The moment Rosie identifies a suspicious expense, she generates a *tweet* in a neutral tone for congresspeople and citizens to contradict or confirm the reported information. Jarbas is a platform that accompanies Rosie and allows citizens to consult and verify the information that arrives on Twitter.

Figure 3.7. Rosie



Rosie
@RosieDaSerenata

A Robô da Operação Serenata de Amor. Analisa e identifica suspeitas em gastos de deputados federais em exercício de sua função.

República Federativa do Brasil serenata.ai Joined January 2017

564 Following 40.8K Followers

Rosie @RosieDaSerenata · Mar 4
🚨Gasto suspeito de Dep. Julian Lemos (PB). Você pode me ajudar a verificar? jarbas.serenata.ai/layers/#/docum... #SerenataDeAmor
9 30 130

Rosie @RosieDaSerenata · Mar 3
🚨Gasto suspeito de Dep. Coronel Tadeu (SP). Você pode me ajudar a verificar? jarbas.serenata.ai/layers/#/docum... #SerenataDeAmor
1 12 82

By the end of 2021, Rosie and Jarbas allowed detecting more than 8,000 reimbursement requests worth approximately USD 680,000. Since they began operating, it is estimated that Congress members' expenses have been reduced by 10% (Cordova and Gonçalves, 2019).

3.3.4. Social network analysis and data mining

Social networks generate, provide and enable sharing data that plays an important role in the fight against corruption. Through data mining, patterns or relationships can be discovered, particularly by cross-referencing different data sources such as; electronic transactions; bank records; employer reports; vehicle purchase statements; and, posts made on social networks, among others.

A famous case illustrating this type of analysis occurred in Colombia, when the young daughter of a customs official posted consumption patterns on her social networks that did not correspond to her father's income level or the university life she apparently led. The official in question was found guilty of collecting multi-million-dollar bribes to allow the operation of a smuggling network in the commercial port of Buenaventura.

Colombia's case was the product of human labor in analyzing information within the internet and cross-referencing different sources. However, this work can be automated. For instance, through its **Connect** system, the UK's HMRC[63] uses social network analysis and data mining to cross-reference companies and individuals tax records to uncover fraudulent or undisclosed activities.

Connect filters large data volumes to detect relationship networks to recover millions of pounds lost by tax authorities as a result of undeclared economic activities (Houlder, 2017). Its predictive algorithm identifies individuals most at risk of committing tax fraud and helps design preventive actions through behavioral *nudges* (Santiso, 2019). For example, HMRC uncovered tax evaders after they appeared on an episode of a TV show spending thousands of pounds of undeclared income on lavish family weddings. Significantly, researchers also investigated their Facebook, LinkedIn, and Twitter accounts.

[63] Acronym for United Kingdom Treasury: Her Majesty's Revenue and Customs.

3.3.5. *Machine learning* and textual audit analysis

The *Analisador de Licitações, Contratos e Editais* (ALICE, by its Portuguese acronym) is a tool developed in 2017 by Brazil's Comptroller General of the Union (CGU, by its Portuguese acronym) to analyze national public procurement and its documents. ALICE takes information from the country's public procurement system (Comprasnet, run by the Ministry of Economy), downloads procurement process documents and generates a report of timely alerts based on its risk assessment of the processes.

The volume of information produced is huge and the CGU faces many challenges to adjust their control to the speed with which public spending materializes after each new contract. According to the entity, an average of 250 notices are published daily on **Comprasnet**, and in the last two years, more than 234,000 bids amounting to over USD 22 billion were managed through this platform. CGU chose to generate a risk assessment system based on a machine learning application called textual analysis.

ALICE uses the text from documents posted on **Comprasnet**. Text classification models work by assigning categories to the data according to content: detecting topics or themes, identifying keywords and names (either buyers or suppliers), to determine the contract profile. It then detects word combinations that might make a contract riskier or deserving of greater attention due to its amount, subject matter, procurement entity or time frame.

Daily, ALICE selects contracts containing text considered strategic by the CGU. After that, an automatic system is activated that sends e-mails to the auditors informing them of those posing greater interest for analysis. Additionally, daily lists and identifying data are stored in a centralized database. Between 2018 and 2019, ALICE analyzed contracts amounting to about USD 900 millions from which about USD 600 million were revoked by the CGU thanks to the platform[64].

The CGU has developed a concept for **preventive auditing of contracts** which relies on artificial intelligence and reduces the time and steps required to exhaust the processes developed by auditors. With the reports sent by ALICE, and based on risk factors from their own experiences, the auditors decide which bids to examine. Each auditor then meets with the entities to assess and validate the identified risks and then prepares and submits a preliminary report to which the entity responds by documenting the actions it has taken to mitigate corruption risks. The response is then monitored by the CGU. According to information provided by that entity, this approach allowed correcting course on contracts valued over USD 1,000 million between 2018 and 2019.

[64] Information provided by CGU.

3.3.6. Artificial intelligence and civil society

Product of a collaborative effort between government and civil society, in 2016 Ukraine launched its e-procurement platform ProZorro. ProZorro is a hybrid electronic system based on an open-source model that enables cooperation between the central database and an infinite number of commercial marketplaces that provide front-end access.

The platform has an online analysis module and allows access to all of the procurement process' data. **Between 2016 and 2019, this led to a reduction in corruption bottlenecks that represented savings for the national economy of around USD 2.5 billion** (OECD, 2019). Rapid digitalization and improvements brought transparency and made information on public contracts (an operation representing 15 % of the country's GDP) accessible to any user. Given the volume (4 500 bids per day), close monitoring was required to ensure compliance, fair market access and the principles of free competition and concurrence. In Ukraine, the National Audit Service conducts contract reviews based on a closed list of 35 risk indicators (Transparency International, 2018).

However, not all initiatives that use data for anti-corruption programs are developed by the authorities. Supported by Transparency International, 25 civil society organizations (CSOs) and the community took advantage of open data available in ProZorro to develop a public procurement monitoring system called DoZorro. Initially, CSOs worked to identify risks and that work eventually evolved into DoZorro, a platform that uses *supervised learning* and artificial intelligence (AI) to assess the likelihood of corruption risks in procurement processes (Transparency International Ukraine, 2017).

Because corrupt organizations and officials adapt and reorganize to hide their activities, DoZorro does not use defined formulas or risks, and instead adjusts automatically. The system independently assesses the likelihood of corruption risks in bids and sends them to civil society organizations in the DoZorro community. The activists' findings are then recorded. If the suspicions are correct the software remembers their choice and if they were not, it forgets them (Transparency International, 2018). Through artificial intelligence, the system re-evaluates its own model and recalculates the weight of each indicator to increase its accuracy at identifying new risky bidders thus becoming increasingly accurate at detecting signs of corruption (Kucherenko, 2019).

Additionally, the online platform allows bidders to leave structured comments on the bid, the buyer, other bidders, etc. The party to whom the complaint is addressed must document the proceedings in case there are violations to the procurement process. If there is no reaction, the case may be referred to an expert for investigation. If the violation is validated, an appeal is submitted to the controlling organisms. The complainant has the opportunity to rate the quality of responses from 1 to 5. Bids where the complaint went unanswered or where the satisfaction rate was below 3 are marked as risky and highlighted on the platform. In turn, those bids are prioritized for review by CSOs that oversee procurement[65]. By 2020, DoZorro had uncovered irregularities in 30 000 tenders amounting to an estimated value of USD 4 billion (ODP, 2020).

[65] See https://oecd-opsi.org/innovations/dozorro/. The official DoZorro website is in Cyrillic.

3.3. Closing remarks and policy recommendations

Created in 2018, CAF's Directorate for State Digital Innovation (DIDE, by its Spanish acronym) prioritizes supporting States in building an agenda to use data and digital technologies as a tool in preventing and investigating corruption. This task has two levels of intervention:

1. the first aims to ensure the existence and quality of data with the potential to be processed by data science for anti-corruption purposes (see chapter 1).
2. In the second, the objective is to provide countries with technical assistance to develop platforms that make intelligent use of data science to prevent, detect and investigate corruption.

This allows governments to shift from a reactive to a proactive and predictive (i.e., intelligent) role in decision making and in their execution of corruption fighting programs and policies.

The success and sustainability of a public policy approach, where data technologies are adopted as a device to fight corruption, requires that countries advance an ambitious digital anti-corruption agenda that takes into account the following aspects:

- **In the digital era, the value chain is clustering towards large datasets. Governments must ensure the infrastructure to facilitate this clustering** whether in data lakes or data warehouses, so that data reuse does not face legal or operational barriers to access.

- **• From the above, it is clearly important for governments to invest in generating computing power to train algorithms that use data to prevent fraud** in a myriad of operations and transactions that require their resources. Examples of these are: security payments; licensing; subsidy delivery; and, tax collection.

- **• Governments can take advantage of "data gravity"[66] to better anti-corruption decision making**. The availability of organized evidence left by data infrastructure can also help improve institutional reforms. In the current context, as datasets enlarge, they become more difficult to move. It is therefore cheaper to let the data remain in certain places.

[66] A concept coined by engineer Dave McCrory, who points out that "data attracts more data". See: https://datagravitas.com/

- **Applying international standards and practices to produce, publish and reuse data is a cost-effective alternative for anti-corruption strategies;** for example, the Inter-American Open Data Program (PIDA, by its Spanish acronym) which contains a series of recommendations and measures to produce and make publicly available 30 datasets that can be used in the fight against corruption.

Applying international standards and practices for the production, publication and reuse of data is a cost-effective alternative for anti-corruption strategies.

- Legal and institutional frameworks must be adjusted to create an enabling environment that allows integrity policies to leverage digital technologies and generate results.

    - **Latin America still needs reforms to mitigate corruption, most of them related to the 2018 Lima Commitment.** Institutional adjustments are needed to regulate conflict of interest, and facilitate access to information on this matter. Another pending aspect in line with good practices is the regulation of *lobbying*. This would help to keep formal and publicly accessible records of lobbyists. Implementing unified registries of beneficial owners would improve the effectiveness of anti-money laundering mechanisms as well as anti-bribery conventions (see chapter 6).
    - **Governments must ensure coordination and collaborative environments for data-driven anti-corruption strategies to work.** Different departments or agencies may have reservations about sharing data or changing the way they manage it, perhaps because they interpret such tasks as a relinquishment of the powers or authority granted to them by the constitution and laws governing each country. This has made it difficult for governments to consolidate a coherent anti-corruption data strategy.

Finally, as an essential part of the reactivation programs, it is important to emphasize that the integrity agenda will be decisive for economic reactivation. Reducing corruption risks helps ensure that government spending translates into an effective provision of public goods that enables markets and favors those most economically vulnerable. In this sense, digitally transforming governments is a necessary, rather than a complementary, component of building a digital public integrity agenda.

Box 3.2. Data science to identify corruption risks

In 2021, CAF, in partnership with the Inter-American Network for Government Procurement (RICG, by its acronym in Spanish), launched the first **«Guide for the identification of corruption risks in public procurement, using data science»**.

It is an instrument to enable public procurement agencies interested in taking advantage of digital technologies for data reuse to create intelligent alert systems that warn about irregularities in procurement processes. To this end, the guide develops three aspects:

- Institutional architecture necessary for units within public procurement agencies to incorporate different datasets as input for decision making; contractual risk; management; monitoring; evaluation; innovations; analysis; and, verification.

- Information flows necessary to complemented public procurement data sources with other open data platforms that can be associated with public procurement's different phases and variables. Identifying information flows and data combination facilitates the finding of anomalies in public procurement.

- Identification of early warnings, red flags and risk prioritization, with a brief roadmap for creating a timely warning system with databases, red flags, indicator aggregation algorithms, risk visualization interface, and information analysis and verification.

In Bogota, the aim is to ensure transparency and accountability in projects valued at USD 7.3 billion, such as the construction of the city's first subway line, hospitals, wastewater treatment and road networks (Infrastructure Transparency Initiative, 2021).

Source: Own elaboration.

4. *Blockchain* and its applications in public integrity

“

Once doubt begins,
it spreads rapidly.

J. M. Keynes, General Theory of Employment, Interest and Money.

Blockchain and its applications in public integrity

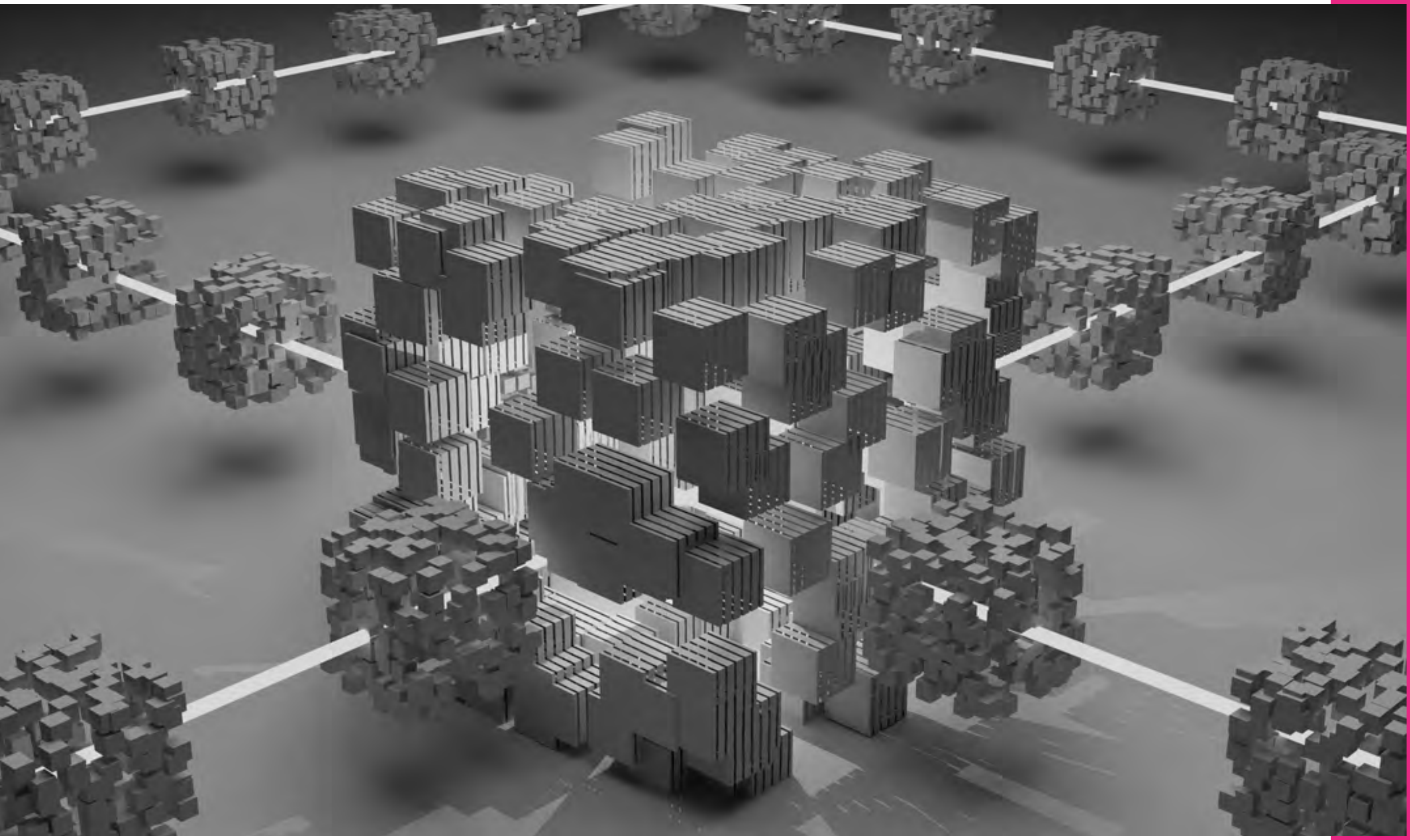
Forgery is a practice as old as paper and writing. For centuries, to transfer rights, property or obligations unlawfully, altering dates, signatures or other characters was all people needed to improperly alter official records. Curiously, not-paper-based tampering remains a problem. The prospect of a world in which all text, audio, image and video data are digitized on easily modifiable media raises the question of how to ensure the integrity of these records; that is, how to certify when and by whom a document, data or file was created or last modified in an open and verifiable manner.

In a world based on physical documents, we used to seal a documentary medium as well as authentication by a notary public. In the digital realm, the problem lies in time-stamping the data, not the medium. To solve this, Stuart Habert and Scott Stornetta (**1991**) developed practical computationally procedures for digitally time-stamping documents so that it would be unfeasible for a user to tamper a document, even with the collusion of a time-stamping service. The technique was based on a cryptographically secured blockchain of information.

The use of money in the digital age, as well as digital financial transactions, explain the origin of another important blockchain feature: the impossibility of creating copies. Information such as text, video, images and other data can exist in many places at the same time. But money, understood as records held by an entity, can *exist only once in one single place* when formatted as information. For this to be possible in the digital world, ensuring that there is no copy of the same money record or that no copies are moved is essential. This way, entities like commercial or central banks have an almost exclusive authority to ensure that money, formatted as information, cannot be copied, tampered or duplicated.

In contrast, *blockchain* is used as an "internet of money," promising users the possibility of transacting directly with each other without intermediation (see chapter 5), that is **without asking a third party for a license to occupy spaces or records**. Something similar happens with the model of **decentralized digital identity** that contrasts with the way digital identity currently works (see chapter 5). Today, having multiple identities for different applications is normal for any digital service user. This generates huge volumes of user data for service providers, which in turn has led to two problems: first, private data is stored and left to the discretion of those applications used by the user; second, as a consequence of the first problem users have no ownership of their data. By contrast, decentralized digital identity is based on the idea that such identity belongs to each citizen and, therefore, it is the citizens who must decide to whom or where to give access to their data through verifiable credentials[67] secured by blockchain and carried on their mobile device.

[67] Decentralized identity works in such a way that, when creating an account, be it work, academic, etc., the user obtains a credential associated with a set of his personal data and which is inserted into blockchain. The developers of this service allow the user to scan an ID and register a photograph of himself, to generate verifiable credentials that he will then use to prove his identity to different platforms and institutions.



Blockchain also offers properties that could help prevent corruption and restore citizens' trust in governments. Although there are no evaluations that systematically determine its effectiveness in reducing corruption, there are case studies that show this technology's potential. For example, Aliyev and Safarov (2019) pinpointed use cases of *blockchain* to **identify cases of corruption and provide transparency in some government processes**.

Based on specific cases that were developed mainly as proof of concept. this chapter explores how blockchain technology works and what potential applications there exist in corruption control. These experiences are a reference for governments to identify processes in which blockchain can be included as a tool for integrity. It is important to note that this technology is relatively new, and its impact or effectiveness in preventing or reducing corruption still needs statistical evidence. In this sense, the chapter is structured as follows:

- First, it explains basic concepts to understand: how *blockchain* works and some of its characteristics associated with transparency and trust in governments' actions.

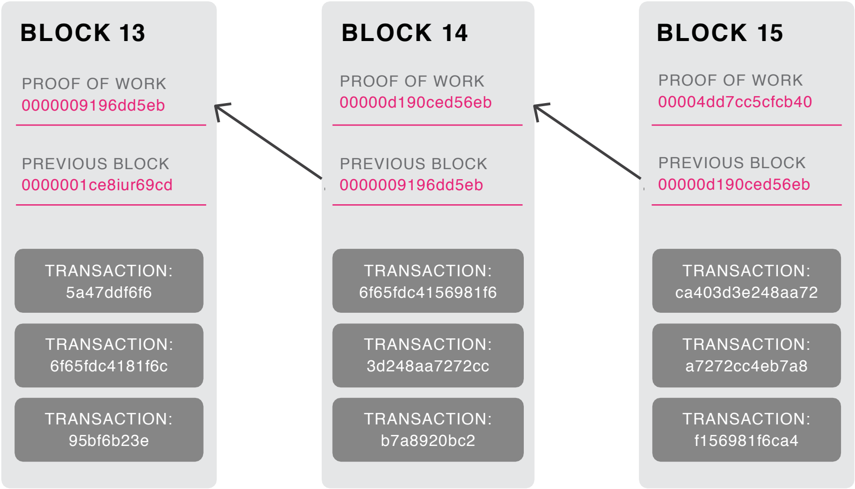
- Second, it presents practical experiences from *blockchain* technology's implementation in the fight against corruption.

- Finally, it proposes a series of recommendations for governments that intend to implement this digital innovation as a tool for integrity.

4.1. Fundamentals of *blockchain*

Blockchain **or digital signatures of information, is a distributed ledger technology allowing transactions to be recorded in blocks.** Each one contains information from previous transactions or blocks thus creating a chain in which every transaction has an immutable auditable trail (see Figure 4.1) and is validated in real-time by all interested parties or "nodes" in a decentralized way (see Figure 4.2). This technique is supported by a distributed public registry that permanently maintains a growing list of fully traceable records or transactions gathered in blocks and secured against tampering **(CIAT, 2018)**.

Figure 4.1. **Illustration of the *blockchain* transaction log.**

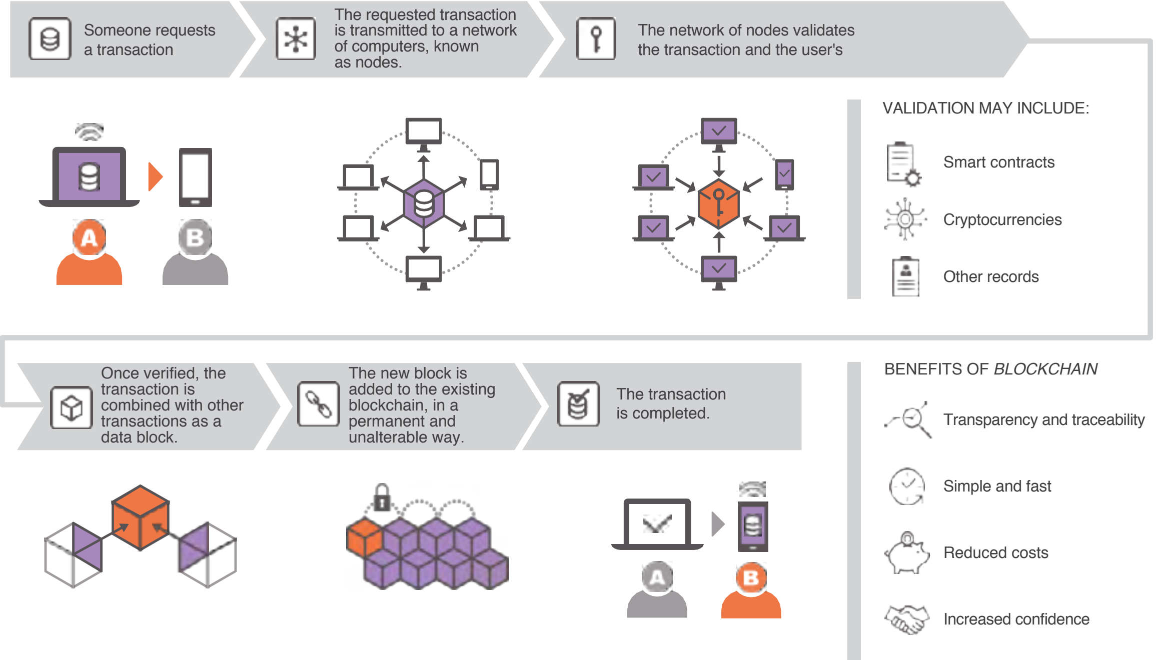


Source: English, M.D., Auer, S., and Domingue, J. (2015).

One way to understand the mechanism that allows blockchain's decentralized operation is to imagine a Google document that does not require Google accounts or a Google-Drive to modify files, and in which each modification follows certain parameters validated by thousands of users. Applying the same intuition to the realm of money was rendered possible through cryptocurrencies. Its developer, who goes by the pseudonym **Satoshi Nakamoto, created a mechanism that registers and modifies information such as the digital currency's** ownership in a decentralized registry that is shared and accessible by millions of computers or members of a network.

These records are tamperproof, that is to say they cannot be erased or hacked, thus guaranteeing their immutability and traceability. What remains in the blockchain registry are blocks of modified information validated by all network members instead of by a central entity. **Millions of members or computing units in a network doing that work** iimply decentralizing the transaction's authentication process. In this way, a blockchain registry accumulates all transactions made and duly validated which cannot be tampered or eliminated. Still, there are different classes of *blockchain* (see table 4.1), with particular characteristics (Aarvik, 2020).

Figure 4.2. **Illustration of the *blockchain* transaction log.**


Someone requests a transaction
A
B
The requested transaction is transmitted to a network of computers, known as nodes.
The network of nodes validates the transaction and the user's
VALIDATION MAY INCLUDE:
Smart contracts
Cryptocurrencies
Other records
Once verified, the transaction is combined with other transactions as a data block.
The new block is added to the existing blockchain, in a permanent and unalterable way.
The transaction is completed.
A
B
BENEFITS OF *BLOCKCHAIN*
Transparency and traceability
Simple and fast
Reduced costs
Increased confidence

Source: Atencio (2020).

Transactions validated and secured with blockchain technology operate under the logic of a smart contract, This concept was coined by Szabo (1996) who considered it feasible to translate contractual clauses into a binding computer programming language. Thus, smart contracts are mechanisms for the automatic execution of obligations foreseen in contractual documents. They use computer codes and avoid resorting to jurisdictional system so obligations or benefits derived from the contract are fulfilled (Padilla, 2020, p. 178).

The simplest illustration of the use of technological instruments to enter into a contract is a soda vending machine[68] that dispenses one dollar worth of beverages. The machine has a stored rule: if it receives a dollar, it must eject the drink. When this happens, the machine *verifies* that it received a dollar (and not, for example, a piece of paper). After verifying that the rule is satisfied, it proceeds to execute: taking the dollar and ejecting the drink. Smart contracts are pieces of information that encode business logic to accomplish three fundamental tasks: storing, verifying and self-executing rules. Smart contracts thus facilitate exchanging money, property, stocks, shares, services, or anything of value in an algorithmically automated and conflict-free manner (**Cong y He,** 2018).

[68] The earliest record of a dispensing machine with such smart contract logic dates back to the year 215 a. B.C. in Egypt, Pneumatika. There, users, by inserting a coin, activated a lever that opened a valve dispensing holy water (Raskin, 2017).

Table 4.1. Different types of *blockchain*

Type		Features
Public	Without permission	The blockchain is public and anyone can participate without permission. Cryptocurrencies such as Bitcoin and Ethereum are an example of this type of blockchain. Since there are many nodes to agree on, they require high network speed (transaction throughput) and scalability (ability to support concurrent users). Some criticisms are related to the high-power consumption required for their operation.
	Authorized	They are open for all to read, but only authorized persons can write records due to oversight from governance control. Since fewer nodes operate within the network security measures are simpler, transaction rates higher and energy consumption is lower. As an example, information about a company's supply chain can be mentioned.
Private	Authorized	Only authorized participants can consult or access the information chain thus reducing the aforementioned costs. They do not require massive decentralization to secure their network because only a few have permission to interact with the ledger, as a result they tend to offer better speed and scalability.
	Authorized	The blockchain is strictly supervised by a unitary central node. It is similar to a traditional centralized database.

Source: Aarvik (2020); OCDE (s. f.).

4.2. *Blockchain* applications to fight corruption

The value of *blockchain* technology in the fight against corruption lies in the fact that its records are decentralized, tamperproof and traceable.. In the public sector, corruption generates distrust between citizens and institutions. Transparency in government decisions and open public records (see Chapter 1) allow monitoring public decisions and contributing to reduce corruption risks through citizen or institutional control mechanisms (see Chapter 2). Blockchain technology goes a step further: it allows the aforementioned records to be tamperproof so that corrupt agents cannot modify, alter or falsify them. According to Santiso (2019), this opens room for potential in processes such as; identity verification; tracking government transfers to citizens; ownership registration of certain assets; and, fairness and integrity in public procurement.

The idea that scaffolds the use of blockchain technology for integrity is relatively simple: **although often absent in humans, incorruptibility of judgment is naturally present in an algorithmic interpreter that has no stake in transactions** (**Wood, 2014**)[69]. In a centralized system, a single authority can maintain the registry and authorize transactions such as; registering real estate titles; entrance into public procurement contracts; and, issuing money. In that sense, if trust in the central node is lost, there would be a generalized failure in the transaction validating system (Davis, Lennerfors and Tolstoy, 2021).

***Blockchain* technology makes records accessible, immutable and secure thus preventing central authorities from acting with excessive discretionality. This allows stakeholders to consult and validate transactions**. For example, in a public procurement process that relies on records documenting compliance with legal requirements, blockchain can trace instances of document tampering such as changes to its terms of reference. It also prevents illegal tampering of biddings and ensures processes visibility for all stakeholders (bidders, public entities and civil society).

Given the existence of different kinds of blockchain, the efficiency of this technology largely depends on its design and the context in which it is applied (Aarvik, 2020). In that sense, before considering implementing this technology in a given process, it is necessary to consider its adaptability to specific public integrity needs (Davis *et al.*, 2021).

[69] In particular, the reliability and integrity of this tool depends heavily on the quality of the code underlying the execution of verification and consensus protocols on each piece of information left on a blockchain.

Figure 4.3. Main properties of the transaction log in *blockchain*

Authenticity and security

Each transaction generates a block of information that has a unique identity and is fully traceable.

Immutability

The information cannot be tampered, deleted, copied or duplicated. Should a block of information be manipulated, all subsequent transaction records are affected and become invalid.

Distributed accounting

Guaranteeing authenticity and control over transactions does not depend on a single or centralized entity, instead it relies on all network users or “nodes”.

Privacy

Transactions are private and the identity of natural or legal persons is not linked to the transaction. This does not mean that users are completely anonymous, but it pseudo-anonymizes them.

Source: Own elaboration.

The OCDE (2018) has identified anti-corruption applications including, among the most noteworthy; human talent recruitment; electronic voting; accountability in public resources’ administration; management of judicial decisions records; and, public procurement. This section discusses some of these applications, including those developed as proof of concept, **which are as a source of reference for governments interested in applying *blockchain* as a tool for integrity**.

4.2.1. Ensuring integrity in public procurement with *blockchain*

Public bidding handled by digital means, such as electronic portals for public procurement, can be even more transparent if blockchain technology is used. This requires government procurement entities to publish and manage public bidding through these networks and to use “smart

contracts" that allow parties to interact with each other. This way, once the entire process has been programmed as a smart contract it becomes tamperproof. For example, Chile phas used blockchain to certify procurement orders to achieve traceability in its governments bidding processes and public procurement.

More specifically, applying *blockchain* to public procurement requires each step of the process to be programmed in blockchain before the bid is published. This allows its records to be immutable and unalterable: both bidders and administrators within the bid follow these steps under the dynamics of smart contracts, i.e., an automatic execution of rules or obligations derived from the procurement process is generated.

Applying blockchain to public bids requires that each step of the process is programmed in *blockchain* before the bid is published. This allows its records to be immutable and unalterable.

By making records accessible, immutable and secure, *blockchain* technology prevents central authorities from acting with excessive discretion and allows stakeholders to consult and validate transactions. For instance, in public procurement, blockchain can ensure a procedure's integrity because all transactions are time-stamped. This makes tampering of the document traceable and prevents illegal changes from occurring. Likewise, queries can be made during the process, irregularities can be reported and clarifications can be requested so that moving forward with the bidding process is unfeasible if, for instance, there is no response to the requests. Moreover, *blockchain* guarantees process visibility for all stakeholders or nodes (proponents, public entities and civil society). Therefore, for corruption to occur, it would be necessary for all nodes to validate or accept the corrupt transaction.

Although there is no systematic evidence on the impact of this technology in risks related to procurement within the public sector, there are cases that illustrate and provide alternatives to design a blockchain intervention in these transactions. The experience of Colombia´s School Feeding Program is described below because it covered the entire public procurement process, and illustrates how to articulate the concepts of blockchain and smart contract to manage public bidding.

Blockchain in the school feeding program (PAE, by its Spanish acronym)

Colombia's Office of the Inspector General (PGN, by its acronym in Spanish) developed a proof of concept to **apply authorized *blockchain* technology** in Medellin's procurement of its school feeding program[70]. *Blockchain*

[70] The School Feeding Program in Colombia (PAE, by its Spanish acronym) is a mechanism that promotes access and permanence in school for children and adolescents of school age who are registered in the official enrollment, through the provision of a free food supplement. The PAE has been recurrently targeted by corruption networks in Colombia (Roseth et al., 2021), so PGN has tried to adopt digital innovations to improve preventive controls (see Chapter 3).

showed applicability in several aspects of public procurement. First, the mechanism pseudo-anonymizes suppliers but does not erase their actions within the bidding process. This makes all bidders known and closes the window of opportunity for irregular agreements between companies or between a bidder and an official to direct the bidding process. Once the bidding terms of reference are publicized, they are tamperproof. The same happens with citizens' comments, which are recorded and cannot be eliminated. This way, the procurement entity's responses also remain registered and unmodifiable in the *blockchain*[71]. The system even prevents making progress in the bidding process if the different bidders' questions are unanswered.

Additionally, when suppliers send their proposals and attached materials, they are received by the procuring entity and anonymously registered in blockchain. In a smart contract mode, proposal cannot be opened until the evaluation process begins as previously programmed. In fact, the public entity is unaware of the proposals origins before starting their evaluation process. Subsequently, it must score all of them because the smart contract mechanism does not allow bidding process to move forward to the award phase without having scored all proposals. This precludes the existence of illicit agreements made in advance of bids to unduly favor a particular supplier. Finally, this pilot adopted a function allowing PGN to receive alerts in case of; tampering to the bidding terms of reference; if communications between stakeholders occurred outside the deadline periods; or, if the deadlines were changed at any point in the process. This would make it easier for the control agency to act in real-time on public procurement processes.

When compared to any other, this technology's added value lies in the decentralization, traceability and tamper proofing of records. In the event of any irregular transaction in the procurement process, records have a traceable and immutable authorship identity. Moreover, for corruption to occur consensus from all nodes in the network is required.

According to the **World Economic Forum, the use of *blockchain*** to fight corruption in public procurement is promising, but it also has important limitations. Among others, these include; supplier privacy and anonymity; uncertainty about scalability; and, agreements between companies outside the platform. Moreover, in Colombia's case it also identified regulatory deficiencies in the use of public *blockchains*.

[71] It is important to clarify that the need to correct the terms of reference may arise, since unintentional errors may occur. The advantage of the blockchain is that the previous version or version with errors is anyway recorded in the registry, as well as the new version, which allows absolute traceability of the process.

Emergency procurement during the pandemic

To contain the COVID-19 outbreak, the governments of the region had to purchase urgent medical supplies such as face masks, ventilators, covid tests and covid vaccines. This type of expenditure is particularly vulnerable to corruption (Cetina, 2020) because the urgency demanded by emergency public procurement trades off with open competition and objective awarding in procurement processes. However, as explained throughout this section, blockchain technology can improve integrity levels in these transactions.

The United States deployed blockchain-based solutions for hospitals public emergency procurement. There, they faced a challenge posed by the existence of around 200 new suppliers of necessary items to address the outbreak. Meeting the urgent supply needs in that context presented two problems: first, it was impossible to contract with all 200 suppliers (or a significant proportion of them) to ensure supply; and, second there was significant urgency for procurement entities to objectively select the most suitable or competitive suppliers to meet hospital needs during the outbreak's peaks. Faced with these conditions' hospitals adopted blockchain technology to guarantee a minimum standard for quality and origin of medical equipment.

In U.S. procurement processes, a mechanism was tested to match procurement entities and market suppliers. Bidders create a profile on the IBM Rapid Supply Connect portal, which is stored in blockchain. Additionally, they upload data such as; financial information; certificates from medical authorities; and, tax IDs that are required by government entities that manage public procurement. Hospitals can then search the *blockchain* for medical equipment and request information about the supplier, which will be provided immediately once the latter agrees to share it.

Blockchain innovations helped make procurement more integral and simplified its selection processes based on innovations such as the following:

- **As a supplier, registration and validation is done only once.** In a conventional public procurement process, suppliers must provide updated information for each contract (licenses, financial solvency and company address, among others). With *blockchain* technology, suppliers update each piece of information as it changes and applies to each State contract, simplifying the process immensely. Since changes remain on the blockchain, all network members validate every change and piece of information thus making the vendor reliable.

- Then this becomes an **assured digital identity** that is very valuable for procurement entities because they do not have to verify the supplier's identifying data.

- The **supplier's suitability and experience** (which generally must be accredited to earn points and demonstrate suitability) is automatically recorded because each transaction or supply contract is recorded and authenticated. Because this information is tamperproof, the procurement entity has no need to request it, instead it can consult it and request new supplies. This request is also recorded in the blockchain. This way, each company and procurement entity's records are stored individually.

- All of the above **reduces room for fraud and lowers entry barriers for new suppliers**. Companies do not see each other's information and proposals so they cannot collude to raise prices artificially. Moreover, although it is not necessarily competitive —since the emergency generally allows direct procurement, the process is automatically directed by an algorithm. Procurement entities register their supply needs, and the platform displays a group of suppliers capable of satisfying it. This allows any new companies entering the registry the opportunity of participating in the supply chain and reduces the opportunity to fix contracts through undue agreements between public officials and suppliers.

4.2.2. Cash transfers

Social transfer programs are particularly vulnerable to fraud, and blockchain technology can be deployed to mitigate these risks. The emergency response has been to implement cash transfer programs (CTPs) to those most vulnerable during the pandemic. According to the UN's FAO and the ECLAC (2020), at least 20 million people fell below the poverty line as result of the health crisis. About 15 countries in Latin America developed cash transfer programs (PTM, by its Spanish acronym) as a result of the pandemic (OECD, 2020). The crisis consolidated the debate on the need for a universal basic income.

However, emergency programs such as these are vulnerable to capture, fraud and corruption. In Colombia, press reports indicated that the **Ingreso Solidario program** was allocating resources to fictitious or deceased people. Argentina had a **similar problem** with the Emergency Family Income (IFE, by its Spanish acronym) program. According to an Argentine deputy's complaint, there was an influx of Paraguayan citizens who crossed the border to irregularly claim the subsidy. In Brazil, the Union's Court of Auditors (TCU by its Portuguese acronym) **detected fraud** in the emergency aid programs. It reported that aid was given to deceased persons, and other ineligible citizens potentially generating an economic loss of approximately US$185 million.

Combining algorithms that develop smart contracts with those that secure information in blockchain is one element that considerably reduced the margin of discretion in those responsible for the delivery of money in the CTPs.

Blockchain has potential to mitigate resource diversion and the aforementioned risks in CTPs. For example, the World Food Program (WFP) developed **Building Blocks** a project to determine the feasibility of incorporating blockchain into CTPs for over 100,000 Syrian refugees in Jordan. This program used a private authorized blockchain (see figure 4.1). The network's nodes consist of organizations participating in the humanitarian response and entities seeking a neutral and transparent space to collaborate, transact and share information securely in real-time (WFP, 2021). This development also represents a digital identity solution for undocumented refugees. Cash is stored in a beneficiary's account and its value and data are validated by different blockchain nodes. Then, based on a smart contract, cash received or spent by the beneficiary is paid through a commercial financial services provider and payments are stored in a *blockchain* integrated with biometric authentication technology[72] so that the WFP has an immutable record of each transaction.

The World Food Program estimated savings of USD 2.4 million as a product of the humanitarian *blockchain* and has invited other UN agencies and humanitarian actors to collaborate on a neutral blockchain network to improve cooperation, reduce fragmentation and strengthen the efficiency of interventions geared towards development.

Combining algorithms that develop smart contracts with those that secure information on blockchain is an element which considerably reduces the margin of discretionality of those responsible for CTPs. Although there are no systematic evaluations on the effectiveness of blockchain in reducing illicit cash transfers in CTPs, the available evidence suggests that this technology can complement others with proven effectiveness, such as biometric authentication (see chapter 2, section 2.1.5). By requiring a decentralized system to validate beneficiaries' identities and transfers or transactions in their favor, it becomes almost impossible to generate payments to fictitious, deceased or ineligible persons. Even in the event of it happening, blockchain would allow tracing what happened to those resources thus facilitating tracking and ultimately recovering funds.

4.2.3. Supply chain integrity

Mass vaccination against COVID-19 presents an unprecedented challenge to the region's governments, particularly in the distribution and administration of vaccine doses under a targeted equity criteria, It has also required striking a balance between personal data protection and the use of personal

[72] The effectiveness of biometric authentication in PTM was tested by Muralidharan et al. (2016). For more details, the reader is referred to Chapter 2, Section 2.1.5, of this report. There are no similar studies verifying the effectiveness of a technology such as blockchain in PTM to, for example, reduce illicit or fictitious payments for.

information to track the pandemic and protect collective public health rights (European Council, 2020). The UNODC has also reported corruption acts such as counterfeit vaccine markets, vaccine theft across distribution systems, and vaccine distribution programs that are plagued by nepotism or political favoritism.

Overcoming these challenges requires integrity in the vaccine supply chain, an area in which blockchain technology can help. In 2019, in the United States, IBM and the Food and Drug Administration (FDA) worked together with KPMG, MERCK and Walmart using blockchain to design a pilot program to identify and track the distribution of prescription drugs and vaccines within the United States. By that same year, approximately half of the country's population had a prescription. This generated the need to improve transparency and trust in the drug supply chain through innovative approaches (FDA, 2020). In order to address those challenges, a pilot project integrated blockchain technology to replace the fragmented and manual notification processes for drug recalls by generating a common record on immediate alerts on the matter (Treshock, 2020).

When combined with a hybrid cloud, blockchain technology allows the creation of an intelligent distribution chain, in which doses are monitored in real-time and their allocation is optimized. In the United States, the experience of the drug distribution project is used in to verify the quality, origin and distribution of COVID-19 vaccines. An authorized private blockchain was implemented to verify the aforementioned vaccine conditions[73]. Blockchain's immutability and distributed de-centralization prevent tampering with data on the delivery and administration processes. This way, because the registry is accessible by the authorities, any potential risk of corruption in the vaccine supply chain is identified, and "black spots" where illegal activities can take place are eliminated. An instance of such activities is the use of political

[73] UNODC has documented corruption phenomena capable of affecting public health objectives, and suggests measures to reduce these risks.

power to evade vaccination schedules by prioritized stages. At the same time, the confidentiality of personal data is guaranteed (Council of Europe, 2020). The latter allows all stakeholders to know and verify information in real-time related to vaccination under criteria of information security and vaccine transparency.

4.2.4. Integrity in financial flows

An authorized private blockchain was implemented to verify the aforementioned vaccine conditions. The characteristics of the blockchain (immutability and distributed decentralization) prevent manipulation and adulteration of data about the delivery and administration process.

Blockchain technology has also been deployed to strengthen the integrity of financial flows. Those who obtain assets through corruption generally have to legitimize the illicitly obtained income through money laundering, whereby the illicit proceeds end up mobilized through the international financial system. For this purpose, shell companies that do not carry out operations of their own but that appear legal are often used to mobilize resources in the financial system without giving indication of their fictitious nature. Something similar happens in corporate schemes used for tax evasion, in which funding flows are moved between front companies to evade the jurisdiction of tax authorities.

This way, regulations aimed at counteracting this crime require financial intermediaries in order to develop policies that allow agencies to develop Know Your Client (KYC) standards and to know their resources' origin and destination (Anti-Money Laundering, AML). However, evidence documented by the World Bank suggests that, in pursuing such policies, financial systems end up rationing services to companies, market segments, and even entire countries that appear to have a higher reputational risk and produce low profits. There is a widespread practice of reducing integration risk by denying financial services to significant customer segments instead of judging the risk based on individual discretionary assessment. According to the World Bank, the adverse effects of these practices fall on the most vulnerable populations, who are consequently excluded from credit markets and formal funding flows.

Blockchain technology can help mitigate risks that affect financial transactions' integrity. For example, Santiso (2018) notes that creating tamper-proof business records would help define beneficial owners and prevent money laundering. Ramachandran and Rehermann (2017) show how this technology reduces compliance costs and increases transaction transparency.

Blockchain, in particular, has the potential to reduce compliance costs associated with KYC requirements[74]. For example, it allows a customer to

[74] A Thompson Reuters survey found that KYC activities cost, on average, USD 60 million per year for financial institutions.

register a “block” by entering most of its own data required for KYC and AML compliance. That information is then encrypted and stored in blockchain (Ramachandran and Rehermann, 2017). Banks themselves could be the validating nodes of information registered by a client. That way clients will have to be consistent in all their information and will therefore be unincentivized to register different versions of their information (economic activity, company name, controlling companies and origin of resources, among others) in different entities (Niforos, Ramachandran and Rehermann, 2017). Moreover, each time a bank incorporates a new client, a representative of that financial entity could access the user’s KYC information without having to requesting it and then verify each new piece of information. This way, customers identity evolves over time as it accumulates and transfer assets, or changes its powers of representation of natural or legal persons.

In terms of money laundering prevention, blockchain’s potential follows KYC’s[75] line by providing a decentralized certification authority that is able to maintain identities and map transactions. The potential positive impact of this innovation has broad implications for a range of financial services including trade finance or cross-border payments. A blockchain identity system will enable end-users to; own and control their personal identity, reputation, data and digital assets securely and selectively; to disclose their data to counterparties; log in and access digital services without passwords; digitally sign claims, transactions and documents; control and send value on a blockchain; and interact in the marketplace through applications and smart contracts. All of this will facilitate more effective oversight by financial regulators, law enforcement and tax administrations.

4.2.5. Land titling records

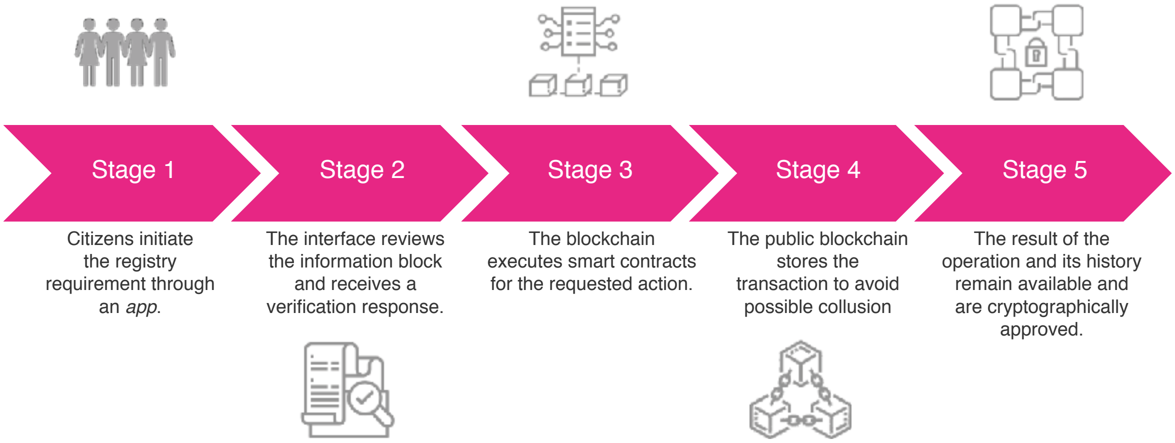
In addition to government transactions, blockchain technology is used to strengthen public records’ integrity, particularly that of land ownership records. State titling registration systems have an important relationship with access to formal credit, higher land values, land investment and income (Feder and Nishio, 1999). **However, in practice, registration systems are inefficient, and generate significant corruption risks** (Van Niekerk, 2021). According to Transparency International, 20% of real estate registry services users declared paying a bribe to carry out a procedure or to obtain information. In other scenarios, the shortcomings of the system itself are used to register assets resulting from corruption.

[75] *Ibidem.*

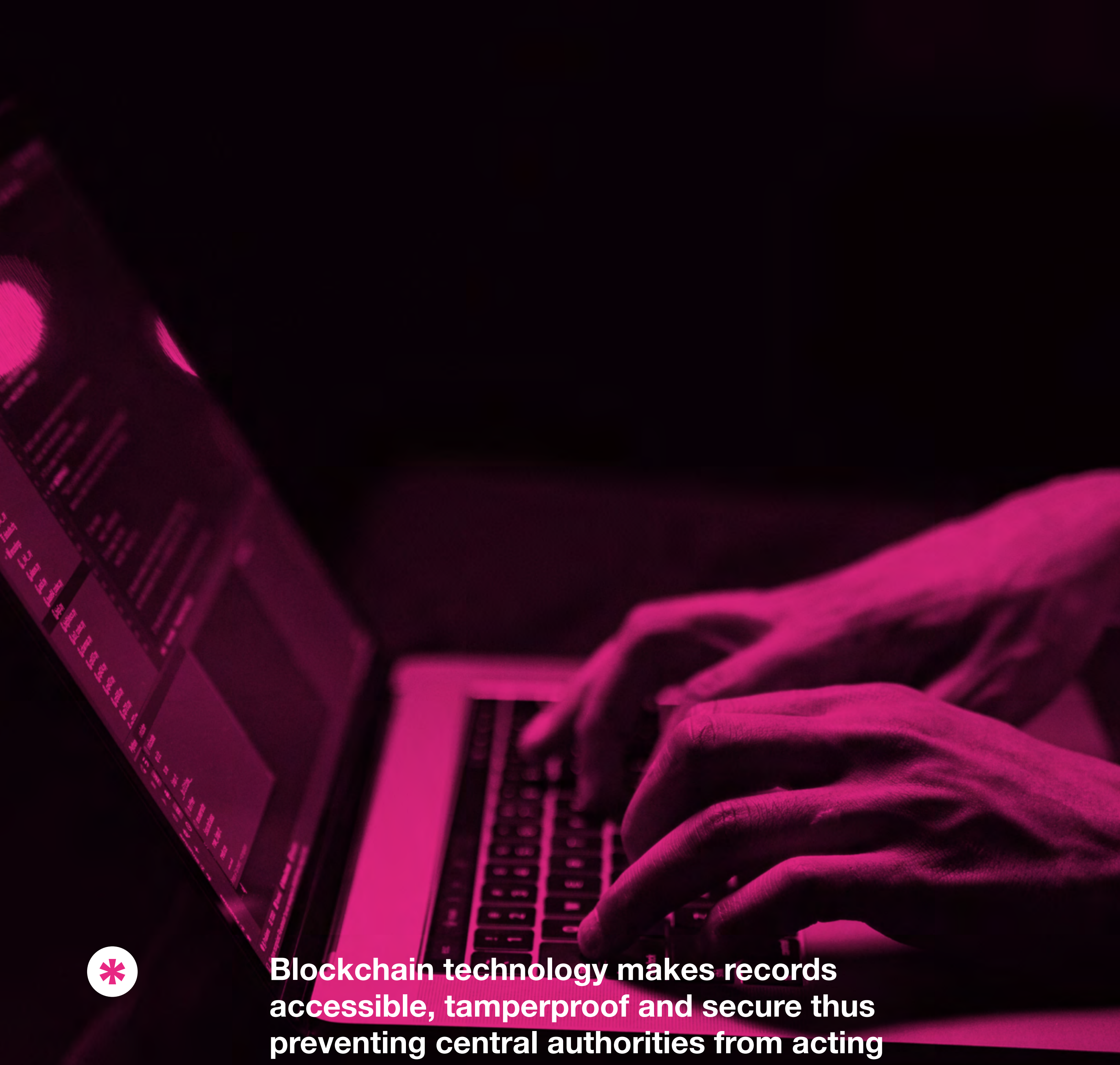
Blockchain technology can optimize public registries, reduce inefficiency and increase transparency levels in areas such as those related to real estate acquisition, permits, concessions and certificates. Countries such as **Brazil**, the **United Arab Emirates** and **Georgia** have bet on blockchain's tamperproof nature and its real-time verification of property rights as a solution to improve their property registration and transfer systems (Graglia and Mellon, 2018). Recently, **Colombia's government** announced the development of a pilot project to adopt blockchain technology in land titling processes in order to **prevent corruption** evidenced since 2012.

In the Republic of **Georgia**, we found a case illustrating how blockchain-based land titling process works. A digital database containing property registration, title deeds and satellite photographs of real estate was created through a collaboration between Georgia's National Agency of Public Records (NAPR), its State Properties Commission (SPC) and its Building Land and Lease Inventory of Property (BLLIP). The system reduced registration costs to less than 0.1% of the property value and delays to one day. However, to solve the crisis of trust in government agencies, a pilot project was launched in 2016 to enable land or real estate registration through an authorized public blockchain based on the existing digital registry (NAPR). This reduced registration transaction time to 10 minutes76. It starts with an app generated citizen registration request. The interface reviews the information block and receives a verification response. Next, the blockchain executes smart contracts for the requested action and stores it to avoid collusion. The transaction's results and its history remain available and cryptographically approved (see Figure 4.5). By **2018, more than 1.5 million property titles had been made public through *blockchain* technology**, improving citizen trust in government (OECD, 2019; Shang and Price, 2019).

Figure 4.5. ***Blockchain-based* land titling registration process.**


Stage 1
Stage 2
Stage 3
Stage 4
Stage 5
Citizens initiate the registry requirement through an *app*.
The interface reviews the information block and receives a verification response.
The blockchain executes smart contracts for the requested action.
The public blockchain stores the transaction to avoid possible collusion
The result of the operation and its history remain available and are cryptographically approved.

Source: Shang and Price (2019).



Blockchain technology makes records accessible, tamperproof and secure thus preventing central authorities from acting with excessive discretionality and allowing stakeholders to consult and validate transactions.

p 137

4.3. Closing remarks and policy recommendations

The properties of blockchain technology (immutable registry and decentralized transaction validation scheme) and the experiences studied in this chapter **show its potential as a technological innovation capable of tackling corruption and restoring public trust in State agencies. However, it is still necessary to generate statistical evidence on impact evaluation and assessment on the effectiveness of blockchain** to reduce specific types of corruption. In this regard, it is important for the different initiatives that use this technology for matters of public integrity to have mechanisms that evaluate its impact and its cost-effectiveness.

It is also important to keep in mind that blockchain is not a tool that should be indiscriminately applied to every transaction where governments need to ensure integrity. The examples shown in this chapter demonstrate a potential that, as a proof of concept, opens room for new disruptive public policy discussions regarding which technological innovations are best suited to improve governance and to fight corruption in the future. For instance, registration of final beneficiaries are new areas where blockchain could forever change the way governments fight corruption that resorts to falsification and the tampering of records for private gain.

In this regard, governments that aim to explore *blockchain's* potential should take into account the following aspects:

- **This is not a technology for storing or securing databases. Preserving their quality and integrity is a fundamental input not a product of the blockchain.** Database quality and integrity are necessary to deploy *blockchain's* potential as outlined in this study. For example, to implement cash transfers (CTPs) the beneficiary databases were safeguarded and secured by the World Food Program. In Colombia's case to implement blockchain in the School Feeding Program (PAE), the database that stores the documents of the contractual process remained in an archive called InterPlanetary File System (IPFS)[76].

- **Government records must correspond to the reality captured by their data.** Generally, for the anti-corruption agenda to succeed an agenda intended to ensure data quality and structure (see chapter 1), as well as communication between different information systems is necessary.

[76] Acronym for InterPlanetary File System, which stands for a system and network designed to store and share information in a distributed file system (https://ipfs.io/).

- **Using blockchain also implies rethinking State procedures, such as public procurement or land titling.** Thanks to the properties of blockchain, this implies redesigning and eliminating several procedural stages or interventions by officials that would be unnecessary. Consequently, the adoption of blockchain in government procedures highlights the challenge of adapting existing legislation and procedures.

- **It is important to formulate a strategy to invest resources in infrastructure for greater computing power** because it is necessary to incorporate nodes and units validating transactions that perform complex calculations. Moreover, the considerable **energy consumption** required for this technology's correct use —derived from the operation of thousands of servers that validate transactions under proof-of-work algorithms—, must be considered as an important cost in deciding in which cases blockchain's use is rational.

- **In order to take full advantage of blockchain's potential to prevent transaction fraud, governments need to move forward on other complementary fronts, such as digital identity.**

- Likewise, successfully implementing blockchain technology or any other technology aimed at contributing to the fight against corruption depends on **citizen education and participation**. All stakeholders must know and understand the purpose of this technology and why it is being used in a given procedure or intervention.

- **Because it can be vulnerable to cyber-attacks and spamming, this technology's risks and limitations should be considered by governments before adopting it.** Additionally, blockchain does not capture the universe of human interactions taking place offline, including bribery or unfair deals. As noted in **CAF's (2019) report on integrity**, if institutional and cultural environment rewards such behaviors, there is little that technology can do to prevent corruption.

5. Risk management

“

It’s not faith in technology.
It’s faith in people.

Steve Jobs

Risk management

At the end of 2020, the city of **Tulsa**, Oklahoma (population of just over 400,000) made the top ten list in the **U.S. Center for Digital Government's** (CDG) most recent digital cities survey. According to the survey, over the previous year, Tulsa invested in modern data solutions through its Urban Data Pioneers program, which applies data analytics to enhance response to critical issues. These improvements can be seen, for instance, in predictive models that identify house fires' risk, or the use of Tableau to help city agencies better understand their finances and make fiscally informed decisions.

However, less than six months after being awarded, Tulsa was victim of a **cyberattack** that suspended most of its digital citizen services and forced the city to shut down its network by disrupting municipal email communications and online bill payments. According to a press release issued by the city government, approximately 19,000 files, including thousands of Tulsa police citations, were stolen last May 2021 and then shared on the **dark web** earlier that same week.

Tulsa's case illustrates a noteworthy occurrence: **while digital transformation brings significant benefits, it also increases exposure to various technological risks arising from an interconnected digital ecosystem.** If these risks are not managed by governments, it could generate costs potentially equivalent to corruption. Some of these cases could be identity theft, tampering with information and sabotaging its availability and, even the abuse of public officials to traffic personal data, privileged tax information and, engage in money laundering. All the above presents a complex outlook of risks in the adoption of digital technologies for public management in general, and for integrity in particular.

The CDG's survey shows how digitally transforming States can strengthen public integrity and, as a result, countries institutional development. However, the digitalization processes of governments, discussed in chapters 1 and 2, and the specific technologies described in chapters 3 and 4, —with important applications in the fight against corruption, are also exposed to criminal activity and misuse which can undermine their potential in public integrity policies.

This chapter presents some risk typologies associated with the development of anti-corruption technologies, and proposes recommendations to mitigate them and achieve effective digital integrity. It is important to point out that the risks identified in this section do not comprehend an exhaustive list, but rather respond to a prioritization of aspects that need to be managed with greater urgency to effectively implement digital innovations in the fight against corruption.

This chapter presents some risk typologies associated with the development of anti-corruption technologies, and states recommendations to mitigate them and achieve effective digital integrity.

- **First, the chapter addresses digital transformation challenges as related to the adoption and protection of digital identity.** The development of digital government platforms and initiatives has paid considerable integrity dividends (see Chapter 2). However, providing better digital services for citizens implies having reliable mechanisms for authentication and identity verification. As we will see, this is not merely a matter of assigning a username and password. Instead, it involves compiling the large amount of data that makes up a citizen's identity and that needs to be secured and safeguarded. This security protects citizen services from fraud perpetrated through acts such as identity theft or the creation of synthetic identities. Digital services increase integrity in the provision of services to citizens, but this does not mean that digitalization by itself is exempt from misuse and fraud.

- **Second, this chapter analyzes risks associated with privacy and use of personal data.** Applications of digital technologies that prevent and detect corruption through descriptive pattern analysis and network analytics (see chapter 3) require the input of large amounts of sensitive data, such as personal and work addresses, blood ties, marital status and transactions. Similarly, operating digital government platforms requires a large amount of personal information in order to successfully build the digital identity that enables services to citizens. In the public integrity eco-system such digital developments such as those require managing risks arising from the misuse of personal data. It is not only a matter of protecting a citizen's right, but also of protecting governments' assets —such as citizens' data— which is managed for specific purposes to safeguard public interest[77]. En ese sentido, abordaremos la importancia de la privacidad por diseño en las plataformas, y del desarrollo legal para proteger los datos personales en usos indebidos, que podrían ir desde la suplantación hasta el tráfico para monetización no autorizada de los datos en publicidad dirigida.

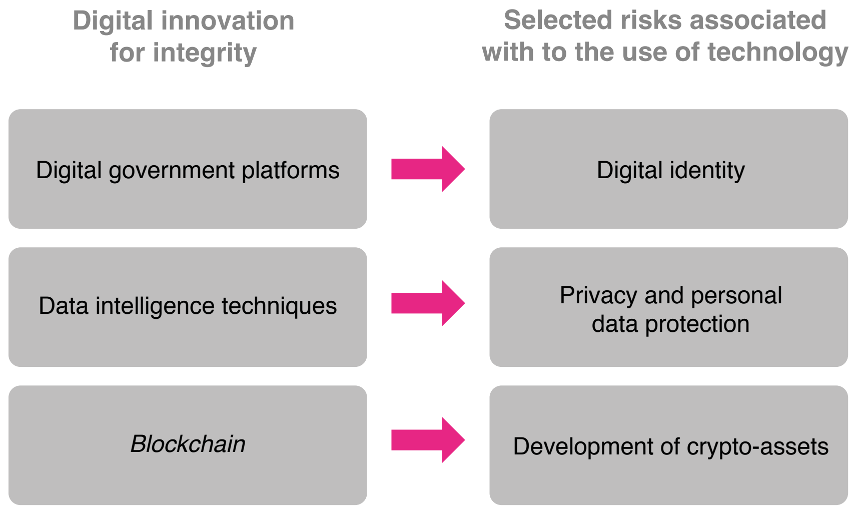
- The **third** section of the chapter **extends the analysis of blockchain use to the development of crypto-assets** which represents considerable integrity risks. The encryption and validation of blockchain, a source of security and integrity in some public management processes (see Chapter 4) paradoxically facilitates laundering activities, since they allow hiding transactions with financial assets of a digital nature through crypto-assets[78] and private currencies. Laundering control practices used by the financial industry are very difficult to apply in the eco-system that validates crypto-assets transactions.

[77] Think, for example, of tracking apps to contain the COVID-19 pandemic, or identity registration platforms to validate voting.

[78] In this report, the term crypto-assets is used as a substitute for the concept of cryptocurrencies, since they do not necessarily fulfill the simultaneous functions of money: store of value, unit of account and means of payment. Nor is the concept of digital currency used, since the latter is the electronic form that money can take, duly backed by an authority such as the central bank..

Finally, the chapter proposes some enabling conditions and recommendations for a digital agenda in the fight against corruption that is aimed at mitigating the identified risks and ensuring the success of digital innovation within the public integrity agenda.

Figure 5.1. Digital anti-corruption innovations and their associated risks


Digital innovation for integrity
Selected risks associated with to the use of technology
Digital government platforms
Digital identity
Data intelligence techniques
Privacy and personal data protection
Blockchain
Development of crypto-assets

Source: Own elaboration.

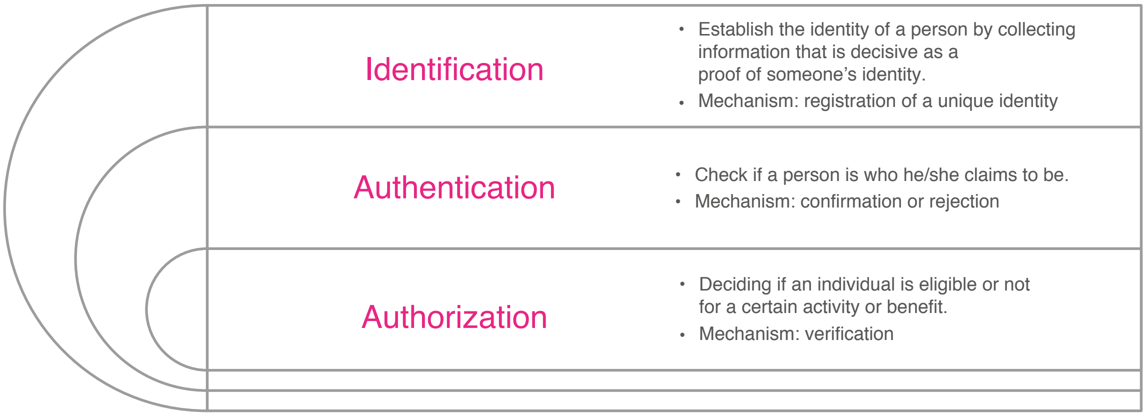
5.1 Digital identity and risk management

The concept of **"digital citizenship"** arose as a result of States' need to provide citizen services through non-presential channels. It also stemmed from governments duty to create and use tools for remote identification and authentication of citizens when requiring digital identity, digital signatures or digital payments.

This tool has also shown its potential in the fight against corruption (see chapters 2 and 4) when running some government services. For example, in Nigeria, the system for digital identification and payment of public officials' payrolls identified more than 43,000 "ghost workers" and generated savings for the State in 2011 (Gelb and Clark, 2013). However, adopting this technology is not exempt from risks, which in turn generate new design and implementation challenges (Beduschi, 2021).

Identification corresponds to the combination of characteristics or attributes of a person that make them unique in a given context. Identification systems have several purposes: *authorization*, *authentication* and *identification* (see Figure 5.2). For several reasons, these are crucial tools for countries development. First, they facilitate interaction between individuals, government and private entities. Second, they enable governments to make decisions more efficiently and to provide better services. And third, they increase transparency in government actions (World Bank, 2014). Therefore, in addition to being a right, ensuring the identification of all people constitutes a **sustainable development objective (16.9).**

Figure 5.2. Basic purposes of identification systems



Identification
- Establish the identity of a person by collecting information that is decisive as a proof of someone’s identity.
- Mechanism: registration of a unique identity

Authentication
- Check if a person is who he/she claims to be.
- Mechanism: confirmation or rejection

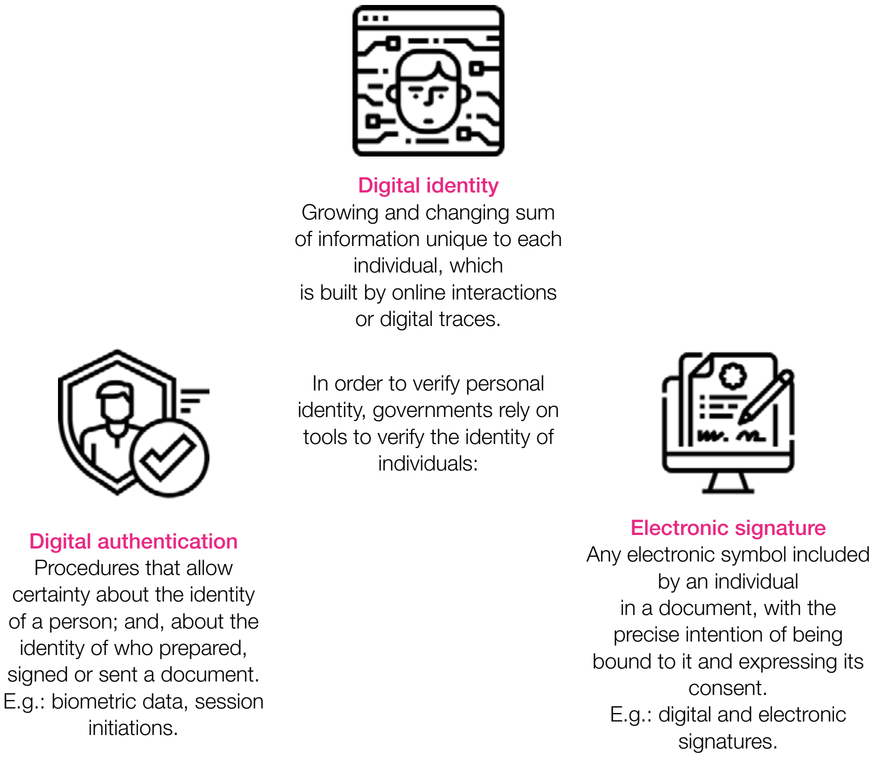
Authorization
- Deciding if an individual is eligible or not for a certain activity or benefit.
- Mechanism: verification

Source: World Bank (2019).

From the digital point of view, identification begins when a user initiates a relationship with an institution or company by incorporating data on their profile registry, as well as their activity and digital services consumption. To do this, the user is identified and a mutually beneficial relationship is built between them and the platform being used. Digitalization’s rapid growth, coupled with the latest technologies and new user behaviors, reevaluate the role of digital identity in the provision of remote services. This is because digital identity allows remote access to banking, government benefits, education and many other critical services (authorization), which require the verification of data proving that an individual is indeed the person they claim to be (authentication).

In the digital world, identification, authentication and authorization activities are not exhausted by assigning usernames and passwords. For instance, elements such as; physical characteristics; financial and tax information; purchase histories; legal and medical records; and, credit history (OECD, 2019) make it possible to assign an identity, with certain attributes, to a specific person. This implies that digital identity is created over time through interactions that produce digital traces or histories of personal data and online behaviors. However, like any technological development this one is also accompanied by risks. Chief among them is cyber fraud related to personal and financial information, private life or preferences data.

Figure 5.3. **Illustration of basic concepts related to digital identity.**



Digital identity
Growing and changing sum of information unique to each individual, which is built by online interactions or digital traces.

In order to verify personal identity, governments rely on tools to verify the identity of individuals:

Digital authentication
Procedures that allow certainty about the identity of a person; and, about the identity of who prepared, signed or sent a document. E.g.: biometric data, session initiations.

Electronic signature
Any electronic symbol included by an individual in a document, with the precise intention of being bound to it and expressing its consent. E.g.: digital and electronic signatures.

Source: Own elaboration.

5.1.1. Basic concepts of digital identity

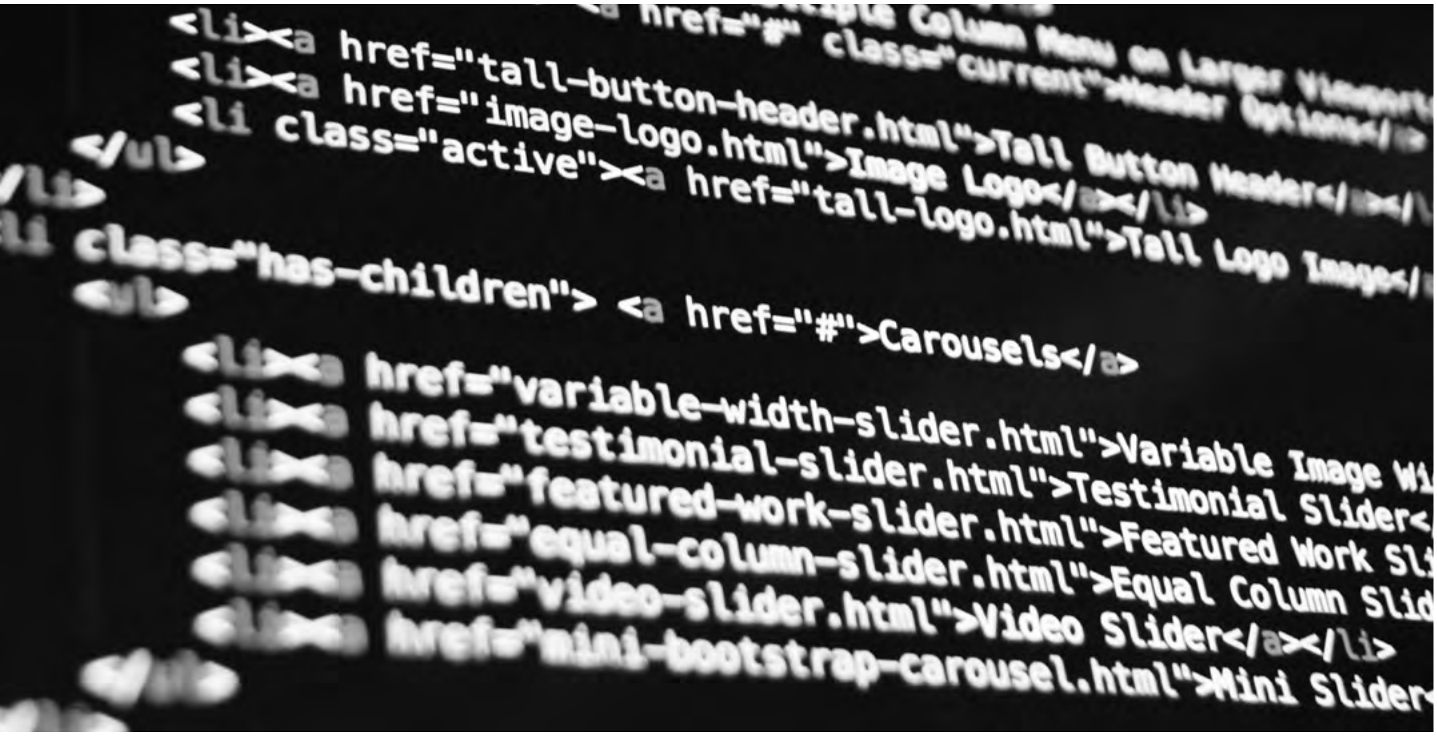
- **Digital identity:** is the sum total of the growing and changing mass of information unique to each individual, their profile and the history of their online activities and transactions. In other words, digital identity is what interactions create over time in the form of digital traces or histories of personal data and online behaviors, such as; financial and tax information; purchase histories; legal and medical records; and, credit history (OECD, 2019). Conceived this way, digital identity is a necessary input to implement technological innovations for public integrity. Santiso (2021) points out some examples that use citizen tracking data and their interactions on different platforms —including social networks, to identify potential tax evaders, as well as the networks behind the Panama Papers scandal. Digital government implies incorporating technologies from their design and conception into government services (see chapter 2, section 2.2). In the use of digital government services (see chapter 2), it is necessary to verify the identity of the citizens with whom the State interacts to deliver goods and services. Digital authentication and digital signatures are used to this end.

- **Digital authentication:** srefers to procedures and tools that verify the identity of the person who has drawn up, signed or sent a document. In other words, authentication allows to verify, for example, that the person who sent a message or wants to access a platform or service is really who they claim to be.

  Traditional authentication involves manual and personal inspection of identity documents to determine their authenticity and the person's corresponding identity. This process is less secure and opens greater room for corruption due to potential human error and high levels of procedural discretion (World Bank, 2019).

  Conversely, authentication can also be done remotely through **digital channels**. There are various tools for digital authentication, for instance, account logins or biometric data (facial recognition or eye or fingerprint scans) to access services and carry out digital interactions. Thus, access to digital profiles is conditioned by authentication tools that make it possible to prove that the person seeking access to a digital service is really the one interacting with the platform.

- **Electronic signature:** **refers to any symbol based on electronic means that is used or adopted by a given party with the precise intention of binding it to a document**. Regardless of the rules established by each country's procedural norms, for electronic signatures to have legal effect,



```
<li><a href="tall-button-header.html">Tall Button Header</a></
<li><a href="image-logo.html">Image Logo</a></li>
<li class="active"><a href="tall-logo.html">Tall Logo Image</
</ul>
/li>
li class="has-children"> <a href="#">Carousels</a>
<ul>
<li><a href="variable-width-slider.html">Variable Image Wi
<li><a href="testimonial-slider.html">Testimonial Slider<
<li><a href="featured-work-slider.html">Featured Work Sl
<li><a href="equal-column-slider.html">Equal Column Slid
<li><a href="video-slider.html">Video Slider</a></li>
<li><a href="mini-bootstrap-carousel.html">Mini Slider
</ul>
```

they must comply with two fundamental characteristics (Rincón, 2020) e.g., (i) the content of the electronic document must not have been tampered with **(integrity)**, and (ii) there must be certainty as to the identity of its author **(authenticity)**.

Implementing mechanisms that comply with both characteristics generates; an environment of full identification and integrity for the document and the need for an authentication mechanism using data messaging. This way, consent is provided through electronic means. Moreover, in some legal systems, a conceptual distinction is made between "electronic signing" as a general category and "digital signature"[79] and "electronic signature"[80] as specific types of the procedure (Rincón, 2020).

5.1.2. Risks related to digital identity systems

Once digital identity is adopted to make the provision of digital government services (or any other in the digital economy ecosystem) more agile and transparent, there is exposure to risks that go beyond the government's digital governance capabilities (see table 5.1). Such risks stem from the possibility that criminal networks find a way to illicitly exploit stored data and generate digital identities. In the real world, for instance, physical contact is required for authentication and signing processes, which imposes a natural barrier to those who impersonate an identity in order to claim money or demand rights (*i.e.*, physically, one can be in one place once and not in several at the same time). However, in the digital world, the same criminal could repeat the impersonation process simultaneously, as many times as necessary, by stealing the data once. This is possible because digital authentication and identity rest on the same pool of personal data that can be stolen or misused.

[79] The digital signature is a mathematical procedure that makes it possible to guarantee the two attributes of electronic communications: authenticity and integrity. In order to have a digital signature, it is necessary the intervention of a trusted third party called "certification entity", which guarantees precisely the identity of the person who appears as the holder of the digital signature. This procedure ensures the authenticity, since it determines the authorship, as well as the integrity of the content of the transmitted data thanks to the intervention of this third party.

[80] For its part, the electronic signature operates without the intervention of a third party. It refers to any symbol based on electronic means, used or adopted by a given party, with the precise intention of binding or authenticating a document so that it complies with the characteristics of a handwritten signature. However, for this signature to be considered valid, there must be an element of linkage with the data message itself sent by the signatory, through which he proves his identity in the digital world. Additionally, it is required that the signatory declares or accredits his will with respect to the content of the signed document. In summary, the difference between electronic and digital signatures is exclusively evidentiary, since the digital signature incorporates authenticity and integrity automatically, while the electronic signature needs to demonstrate compliance with these two attributes.

Table 5.1. Risks of digital identification systems (DIS)

Exclusion		Implementation of DISs that exclude alternative or informal means of proving people's identity generates the risk of further **marginalizing groups that do not have technical skills or access to digital channels**.
Privacy and security breaches		Inherent to the capture, storage and use of sensitive personal data are the **risks associated with breaches of privacy, data theft and misuse, identity fraud and discrimination**.
Links with supplier or technology provider		**Dependence on a specific technology or vendor can result in "blocks"** increasing costs (e.g., software licenses) and reducing the system's flexibility to meet a country's needs as they develop.
Inappropriate or unsustainable technologies		Systems that are **not context-specific or are expensive have failed to guarantee development objectives** and are unsustainable in the medium and long term. For example, some countries have implemented expensive multipurpose smart cards, which are not used by citizens.
Limited infrastructure and connectivity		**Rural and remote areas lack basic ICT infrastructure, mobile connectivity and reliable internet. This can create difficulties when implementing digital identification** systems that require power and connectivity during enrollment (e.g., for data transfer or verification of duplicate biometric enrollment) and for authentication.
Weak public procurement systems		The processes for **DISs procurement and management are complex** due to the wide range of available technologies and the different types of procurements that must be completed. As a result of poor procurement processes and **inadequate management of vendor contracts**, there can be procurement failures, delays (e.g., due to appeals), and vendor and technology lock-in.
Insufficient national cybersecurity capacity		Low- and middle-income countries often have **capacity gaps in their central cybersecurity agencies**, which are necessary to provide a secure environment for DISs.

Source: World Bank (2019).

Adopting the concept of digital citizenship, the Government of Colombia recently created the **Digital Citizen Folder** (CCD, by its Spanish acronym). This initiative acts as a repository of the documents needed by citizens to carry out procedures with public entities and as a gateway to their access. Currently, there are 11 procedures available online. The CCD's expansion to other procedures and services offers immense potential in terms of integrity (see chapter 2, section 2.2), as well as savings in time and money for users and public entities. However, it is also exposed to risks because it is a centralized repository of citizens' data with a single access key (the date that the identity document was issued).

The vulnerability to which digital identification systems can be exposed became evident in Chile. In October 2020, the Digital Identification System, managed by the Digital Development Division of the Presidency of the Republic, was reportedly the target of a cyber-attack (Agencia EFE, 2020). The system operates by generating a **unique password** and biometric identification to carry out various public procedures. This raised alert among authorities and citizens regarding the sensitivity of identification systems and digital authentication processes. Consequently, it exposed some cybersecurity challenges.

Digital authentication fraud

Digital authentication systems must be sufficiently secure to protect personal data and prevent identity theft. To this end, designs that require multiple levels of authentication such as data; confirmation; one-time keys; and, biometrics are desirable. However, it is possible to circumvent authentication systems by stealing personal data that are used in some cases as identity verifiers (dates of birth, present or past addresses, or business credit relationships). This allows an impostor to impersonate a platform user and gain access to its services.

The incidence of crime associated with fraud and identity theft has seen a considerable increase in this decade. PricewaterhouseCoopers's (PwC) 2020 Global Economic Crime and Fraud Survey noted that 47% of companies experienced an incident linked to authentication systems in the last 24 months (PwC, 2020). This has occurred on a global scale. For example, in Europe, 79% of organizations surveyed by the Association of Certified Fraud Examiners reported an increase in fraud levels since the start of the COVID-19 pandemic. These ranged from credit card fraud and phishing to synthetic identity fraud in which an identity is created with the intention of defrauding a company.

In most legislations, identity theft is a crime. It is a type of fraud in which an imposter steals individual information from another person (or an organization) and uses it to obtain a monetary or property benefit. For the victim, identity theft can cause financial and reputational damage, as well as a loss of the

For the victim, identity theft can cause financial and reputational damage, as well as a loss of resources used to avoid the consequences of fraud.

resources used to avoid the consequences of fraud. Identity theft also affects organizations, whether public or private.

Once criminal networks have enough information about an individual, they can take over the identity to extract resources through a wide range of crimes. Among them are; false applications for loans and credit cards; fraudulent withdrawals from bank accounts; fraudulent use of telephone calls; or, obtaining other goods or services such as, telephone line access.

In the United States, the Federal Trade Commission (FTC) tracks consumer fraud and identity theft complaints filed with federal, state and local law enforcement agencies and private organizations. According to its data —and primarily due to a 113% increase in identity theft complaints— there were 4.8 million identity theft and fraud reports received by the FTC in 2020, up 45% from 3.3 million in 2019. Similarly, an Interpol (2020) assessment of the impact of the COVID-19 health crisis on cybercrime revealed that the target of criminal networks shifted from individuals and small businesses to large corporations, governments and critical infrastructure.

In Latin America, it is estimated that this crime grew by more than 400% in 2020 (Acosta, 2021) through e-mails used to tamper documents to obtain government contracts, access financial loans and even make online purchases. Similarly, website impersonation grew by 358%, with 4,353 cases reported in 2020, compared to 951 that were reported the previous year (Acosta, 2021). Additionally, the same report concluded that individuals are not the only targets of cybercrime with respect to identity theft.

Therefore, personal data or by definition digital identity must be protected. Protection is not only a matter of safekeeping the information so it is not targeted by hackers (who are part of the realm of software developers). It also requires an institutional and legal scaffolding, that emphasizes effective accountability for the collection, management, custody and use of personal data.

5.2. Data protection as an element of digital integrity

Advances in digital service systems and big data enable organizations that provide technology platforms to obtain detailed information about user access. This information includes geographic location, usage patterns and even biometric data. For example, in early 2020, Colombia leveraged data on its most vulnerable population and worked with financial entities that have strengths in their digital services to implement emergency pandemic cash transfers without forcing beneficiaries to physically attend banks or to rely on cards as a means of payment.

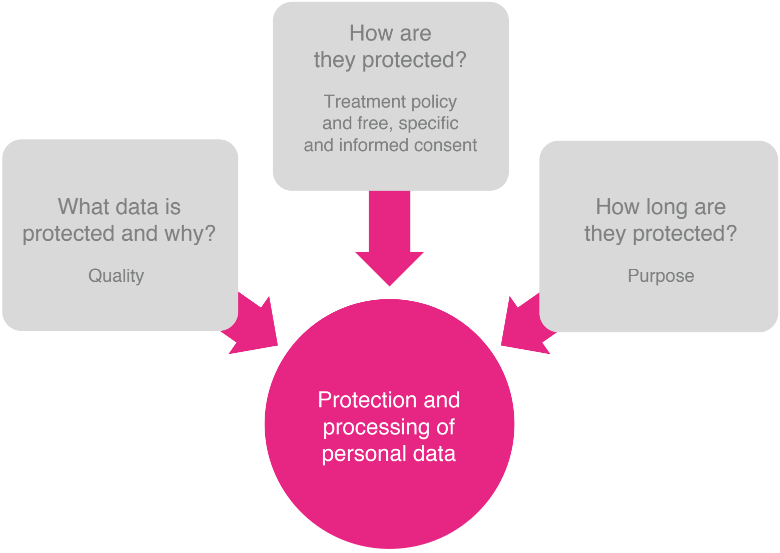
Similarly, massive datasets and analytics on them make it possible to detect corrupt networks and even predict corruption risks. This is in no small measure due to the possibility of digitally identifying individuals and legal entities within structures that could be considered criminal. Even though digital

developments allow procedure simplification; eliminate the need for physical presence; and, apply data analysis techniques to improve processes like the early detection of corruption risks, there are still implicit threats related to the privacy and security of personal data that underlie the use and purpose of these technologies.

The concept of "personal data" includes any type of information about an individual. This can be "objective", such as age, and "subjective", such as the opinions or evaluations made through digital means by such users about a platform or service. The concept of personal data includes information available in any form, such as alphabetical, numerical, graphic, photographic, acoustic, etc. Likewise, it includes paper data as well as any information stored digitally or on videotape, for instance, a sound and image, which are data that can be considered as personal because it represents information about an individual (Koch, n. d.).

"Processing" refers to any operation or set of operations on personal data, whether by; automatic means; collecting and recording; organization and storage; adaptation; alteration; retrieval; use and consultation; disclosure, transmission or dissemination; availability; alignment: combination; blocking, erasure or destruction. In other words, processing (and thus protection) must be present in any operation with personal data performed by the organization. (Wachter and Mittelstadt, 2019). In carrying out these operations, specific issues related to data quality, reasons why data is collected and processing policies must be addressed (see figure 5.5).

Figure 5.5. Aspects that determine data processing


How are they protected?
Treatment policy and free, specific and informed consent
What data is protected and why?
Quality
How long are they protected?
Purpose
Protection and processing of personal data

Source: Own elaboration.

Access and use of these data by unauthorized individuals or for purposes other than those stated at the time of collection can potentially violate the privacy of individuals and cause harm to the owners of the information.

- **What personal data is protected and why?** Within the different classifications, personal data can be divided into e.g., (i) semi-private (financial behavior); (ii) private (home address, e-mail); and (iii) sensitive (personal data, political or religious affiliation, sexual orientation, social status, gender, age, gender identity and health information). From this it follows that the more sensitive the data or the more vulnerable the participants are the stronger the security standards will be. In cases such as these, data storage compartmentalization is advisable. In other words, strictly separating sensitive from personal data is recommended, as is databases encryption. It is also important to specify the methods for data retention.

- **How is personal data protected?** Data processing policies must be periodically reviewed, disclosed and accepted by users, who must express their free, specific and informed consent (Wilms, 2019). Moreover, it is necessary to guarantee the information holders' right to access, rectify, cancel and oppose the provision of their personal data.

- **How long is personal data protected?** The period of data protection and keeping depends on the purpose for which they were collected or processed. When data are no longer needed to fulfill the purpose of their processing, they should be deleted or kept anonymized if they serve historical, statistical, or scientific uses. This way, specific retention timeframes can be determined by indicating the possibility of deleting them once the term has expired. For example, as soon as they are no longer necessary for the purposes for which they were collected[81].

Data protection has become **especially sensitive for countries in the post-pandemic phase** (Cetina, 2021), as is the case of mobile applications used for health counseling or COVID-19 tracking and containment. In particular, there is some opacity about the use that governments will give to citizen data once vaccination achieves herd immunity in each country's population[82].

Throughout this report, we have identified government digitalization processes that are particularly sensitive in terms of personal data, such as public procurement, the provision of social security services and taxation systems. This is because the associated information has a semi-private, private or sensitive nature and, therefore, access and use of this data by unauthorized individuals or for purposes other than those stated at the time of collection can potentially violate the privacy of individuals and cause damage to the information's owners.

[81] In particular, Law 1581 of 2012 constitutes the general framework for the protection of personal data in Colombia. It incorporates the principles and obligations of all those who process personal data to guarantee the protection of the fundamental right to habeas data and the right to privacy.
[82] For example, in China, Alipay and WeChat implemented the Health Code app, used to track coronavirus exposure. As stated by Lei (2020), such companies have asserted their contractual rights to retain the data after the crisis is over, which seems to go against the purpose and objective for which they were collected.

In this sense, treatment of personal data is an essential process in implementing digital strategies against corruption which must guarantee privacy and security.

Risk management in personal data misuse

Privacy

For human beings, privacy is considered a fundamental right that generates a correlative obligation for governments to guarantee an adequate level of protection with respect to an individual's attributed information. EThe government has the obligation to guarantee the rights of citizens with respect to privacy and processing, and to ensure that the personal data is only collected for legitimate purposes (OECD, 2010).

However, its significance and limitations can be assessed by the risks associated to user data in relation to the benefits of partaking in digital world interaction whether it be by using social networks, digital government services or e-commerce transactions. The adoption of technology by users and citizens generates a greater burden for organizations in managing their responsibility to keep datasets secure. Due to these demands for privacy and control, new regulations have been created, such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA).

In general, regulations develop standards and norms that contribute to transparency in the way institutions seek consent for data collection and use, comply with their privacy policies, and manage the data they have collected. In fact, the use of technological platforms involves the exchange of personal information such as; addresses; credit card data; geolocation; travel habits; and, individual preferences related to the use of various goods and personal spaces.

Protecting data privacy implies adopting **privacy-by-design** principles that ensure the appropriate treatment of data used in any action that employs digital platforms. This principle holds that data privacy must appear since the beginning of the planning and design process of digital platforms and services. This implies:

1. **Privacy as a default setting.** From the beginning and throughout the entire processing's cycle, the data controller must have a system with sufficient protection in terms of collection, storage, uses, circulation and access to data. This means restricting shared use, using minimization, eliminating data no longer in use and always operating within a legal basis. It also means using opt-in and opt-out functions and safeguarding consumer information.

2. **Privacy embedded in design.** Information should be understood as another asset in digital services' management. Therefore, like any other asset managed by the State, its protection should be embedded in the information technology infrastructure and processes. In turn, this principle establishes privacy as a core functionality of digital government services. Thus, it is important to use encryption and authentication, and to test for vulnerabilities on a regular basis. No matter whether the process works as it should, institutions must constantly lookout for design flaws in case of a security vulnerability.

3. **Full functionality.** This principle establishes how privacy protection follows data throughout its lifecycle, from collection to deletion or archiving. Encryption and authentication are essential, but there is still more that needs to be done. For instance, only needed data should be collected and it must follow legal basis. When data use is finished, regulatory-compliant methods of deletion and destruction for end-to- end protection should be used.

4. **Visibility and transparency.** Components and operations must be equally visible and transparent to all users. This implies constituting (within the organization's practices) a system that is synchronized with established commitments and objectives. According to this principle, stakeholders should know their privacy and processing practices and share them openly. Thus, there should be a well-written privacy or data processing policy, which is essential in any jurisdiction. It also states that there must be a mechanism for data subjects to voice complaints, ask questions, and request changes.

5. **Respect for user privacy.** Finally, the system must preserve the privacy interests of individuals who provide information. Therefore, it must guarantee sufficient privacy protection measures through appropriate notices related to the use, collection, storage, circulation, and access to data. This last principle means recognizing that, although data is held, it belongs to the user from whom it was collected. Consequently, it is the data subject who can allow and withdraw consent for its use, and not the other way around.

Security

Security of an information system refers to the protection of information and the tools used to prevent breaches and unauthorized access or destruction. Information security, known as cyber or computer security, is a major challenge and a vital component in the relationship of trust between citizens and their governments. Much like identity theft, cyber-attacks can cause economic damage by interrupting information and communication systems and through the loss or tampering of confidential information or other important datasets.

Information security, known as cyber or computer security, is a major challenge and a vital component in the relationship of trust between citizens and their governments.

Security in digital platforms is not a small matter and managing these risks affects both public and private sectors alike. As attacks become more frequent around the globe their relevance has grown. **Forbes** estimates that, by 2025, cybercrime could represent annual global loses world of approximately USD 10.5 trillion, and have significant effects on areas such as the provision of public services like health and transportation. The cost of such crimes can be explained by the scale of the attacks and their perpetrators. The Snowden case exposed a number of breaches and unauthorized accesses to government and private sector platforms in several countries by intelligence authorities (Wright and Kreissl, **2013**). **Sony** cyberattack in 2014 and the **Wannacry** ransomware outbreak have been attributed to North Korea. More recently, the Central Bank of New Zealand endured an attack that gave no clue as **to its perpetrator**; while the attack on the Democratic National Committee in 2016 **has been attributed to Russia**. States themselves are starting to be considered as actors on the risks map related to technological platforms security.

According to Van Eeten (2017), computer security problems come from the Internet's governance and its original conception. ISince its inception, the Internet was not designed with the idea of managing malicious traffic distinctly from benign traffic or to even tell the difference between them. Fidler (2017) points out that defense and intelligence agencies involved in funding and developing the earliest versions of the internet operated under a different threat model: intercepting and monitoring network traffic (i.e., the data being mobilized) which did not consider the subversion of the nodes (network members) responsible for the data. Over time, some threat mitigating capabilities to address misbehaving nodes were added to the basic design of the network itself[83]. However, in terms of security, the authority resided first and foremost with the node owners. In today's context such authority needs to lie with governments.

In Europe, some security and liability standards have been developed for digital governance systems which may serve as a model for Latin America. For example, Directive 2013/40 EU of the European Parliament and Council criminalizes any improper access[84] made with the intention of obtaining an illegal transfer of ownership during the course of data processing (Csonka, 2006). Thus, in Europe, computer tampering involves the unauthorized access and creation or tampering of stored data so that it may acquire a different evidentiary value. Consequently, the course of legal transactions, which is based on the authenticity of the data's information, is subject to fraud and is punishable by law.

[83] Think of blocked ports, anti-spoofing filtering, botnet command and control traffic drowning, DDoS traffic blocking, etc.
[84] It includes the entry, alteration, deletion and suppression of data, as well as interference with the operation of a computer program or system.

Another relevant example is the United States' regulation. Several cases involving fraud and the theft and tampering of confidential information through unauthorized access to computers were motivated by judicial decisions. In 1990, in the case of Estados Unidos v. Schreier, the perpetrators were punished in an exemplary manner for accessing American Airlines' computer reservation system and tampering with its information. The same year, with the Estados Unidos v. Riggs decision, sanctions were imposed because the defendant unauthorizedly accessed Bell South's emergency computer file with the intent of tampering with the telecommunications company's systems and copying subscriber data.

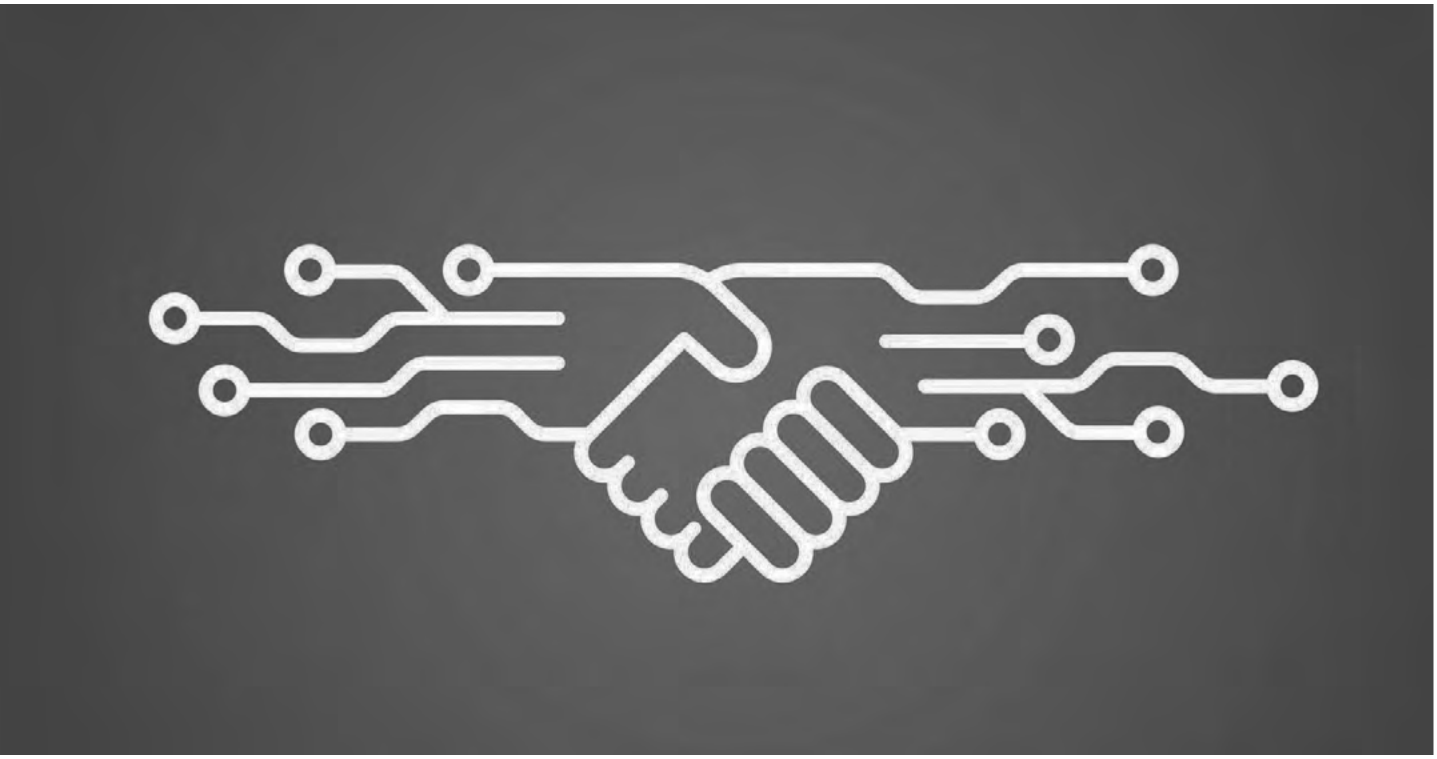
Each of these cases has one thing in common: although the system appears to work, the courts have held that unauthorized access and data copying can be harmful to the data's holders or owners. Therefore, even if the system has not been tampered with, unauthorized data access, alteration or copying of involves a violation of data privacy in the lesser crime.

Among others, in Latin America, violating and tampering with computer systems to receive services and electronic fund transfers by manipulating programs and affecting ATMs are regulated conducts. However, there is no standard for the protection of personal data throughout the entire processing cycle (collection, recording, organization, storage, adaptation, alteration, retrieval, consultation, etc.) or in actions involving unauthorized access to digital platforms and consultation, tampering or extraction of data.

The lack of standards and the role of courts and judges in determining responsibility for the security of digital platforms between users and owners is explained by the fact that there is no benchmark model for digital security governance. Van Eeten (2017) documents that security governance has shifted from device owners to large intermediaries, which means that those responsible for platform's security are no longer the users of computing services or network nodes, but instead the platform's developers. This change is generally associated to benefits such as a more: centralized control over the security of devices and services that reach millions or even billions of users and, therefore, the generation of scale economies for security services provisions.

This trend is driven by an economic rationale: reducing digital services' production costs. When compared to consumers and businesses that own and maintain their own digital infrastructure cloud computing offers considerable efficiency gains. In addition to cost, there is also greater reliability. For instance, Google is more proficient at securing its Gmail platform than most businesses are at securing their own mail servers. In that sense, it is more cost-efficient for governments to turn to large digital service providers for mail, cloud computing and data protection. This means that power has shifted and will continue to shift from device owners to cloud operators and platform and device providers.

The OECD (2011) referrers to these companies as Internet intermediaries and their security practices increasingly determine those of governments and users. The main challenge is that neither governments nor the available literature on digital security propose an adequate way to evaluate the actions of large providers. Usually, cloud operators do not allow audits of their systems and services. With the exception of personal data protection and laws governing the safety of sensitive information for countries' national security, there is a fundamental asymmetry preventing the use of systematic evidence to verify which models, practices and policies are appropriate in this area.



5.3. Risks in *blockchain* technology: crypto-assets and private currencies.

Blockchain technology has in enhancing public integrity (see Chapter 4), because it is based on a distributed consensus protocol and the records it contains are secured against tampering, which generates trust on the activity and security for data generation (Ko, Lee, and Riu, 2018). However, **the decentralized nature of this technology also means that governments are not the only users of blockchain, and that sealing public utility data and records is not its unique application**. Private parties are using this same technology to create and circulate crypto-assets, generating risks that must be considered in terms of integrity.

> The absence of national and international regulation for the adoption of *blockchain* technologies allows the development and expansion of crypto-assets without State controls. Crypto-assets are a form of digital financial asset, that is a digital representation of a value that has not been issued or guaranteed by any central bank or public authority, and that does not possess the legal status of currency or money [...] However, it is accepted as a medium of exchange by legal and juridical persons and can be transmitted, stored and traded by electronic means[85] (Almeyda, 2020).

In current digital innovations from the financial industry's ecosystem such as **FinTech**[86], crypto-assets correspond to digital financial assets based on cryptographic principles and *blockchain*[87], technology, which allow secure, decentralized and distributed economic transactions. It is therefore important to note that they are digital assets not issued by a central authority (in fact, their issuance is open to anyone who wants to develop one) and in which encryption techniques are used to ration currency units and verify the transfer of funds.

[85] Definition corresponding to the German financial regulator, Federal Financial Supervisory Authority, according to Almeyda (2020).

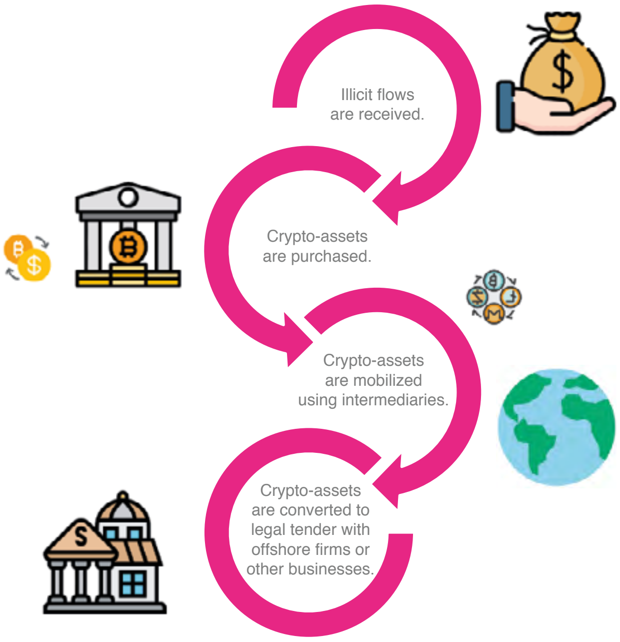
[86] For some observers, the new FinTech ecosystem could replace traditional intermediaries, e.g., banks. However, for other experts, banks and FinTech initiatives have common objectives and could complement their strengths (Arbache, 2020).

[87] Cryptography is used in blockchain technology. Hashing, being the most widely used, is a method of applying a cryptographic function to data, which identifies a data message, of any size (i.e., a file, text or image). In general, it allows to individualize the message and thus to perceive if there were variations; even the smallest change in the input (i.e., a single bit, a single letter or a comma) will result in a completely different hash.

5.3.1. *Blockchain* encryption and money laundering

In recent years, authorities have concerned themselves with the secrecy involved in encrypting crypto asset transactions because it creates opportunities to hide both the origin and ownership of funds. In particular, through crypto-assets, new *blockchain* technologies could facilitate money laundering activities for those who illegally obtain money through corrupt practices such as bribery or the diversion of State funds and income from drug trafficking. According to **Chainalysis**, a firm that specializes in cryptographic forensics, there is evidence of drug trafficking networks converting their funds into crypto-assets then sending them around the world and ultimately converting them into foreign currency. According to its latest report, it is difficult to investigate this activity based on individual cases as well as to capture the resources themselves because when such funds are converted from official currencies to crypto-assets in *blockchain*, there is no trace of their origin.

Figure 5.6. Illustration of money laundering using crypto-assets


Illicit flows are received.
Crypto-assets are purchased.
Crypto-assets are mobilized using intermediaries.
Crypto-assets are converted to legal tender with offshore firms or other businesses.

Source: Own elaboration.

Money laundering is a crime intrinsically linked to corruption. **Just as blockchain technology can be a digital innovation to curb corruption incidences, it can also enable it through crypto-assets, which easily lend**

themselves for money laundering by criminal networks (see figure 5.6). Chainalysis (2021) estimates that, as the overall level of crypto activity increased last year illicit flows accounted for 0.34% of 2020's crypto-asset transaction volume in 2020, compared to 2.1% in 2019. While these figures may seem insignificant compared to those injected into the financial system, the potential of crypto-assets for laundering is still present and deserves the attention of regulatory authorities.

A group of companies dedicated to analytics has emerged to help detect illicit activity in the industry. However, according to the Financial Times, their tools are better suited for detecting crimes that take place on blockchain itself (theft, scams and *ransomware* payments), than for quantifying the amount of criminal proceeds flowing into crypto-financial asset markets. In that sense, available figures may well be underestimated and the problem of laundering through crypto-assets could actually be growing in greater proportions.

5.3.2. Decentralized finance and the inapplicability of due diligence policies

The movement of crypto-assets is made possible by a new industry within the FinTech environment called DeFi (Decentralized Finance). Commonly run on the Ethereum blockchain, DeFi platforms aim to replace financial intermediaries such as banks or brokers with smart contracts, which would automate market activity. Although their legal status is unclear and their structures vary, the appeal of DeFi platforms lies in their potential to reduce costs and speed up trading by using digital financial assets. **The integrity concern is that DeFi's ecosystem competes with and seeks to replace the same entities that governments rely on to enforce anti-money laundering laws** (bankers, brokers and money transmitters) but with the particularity that it does not provide any regulated service, because it does not perform financial intermediation and therefore does not hold funds or custody of the public's money. On the contrary, it is simply an open-source interface for users to interact with their own digital assets.

Thus, for example, DeFi ecosystem platforms are not obliged to request information about their customers or to apply anti-money laundering practices such as Know Your Costumer (KYC). KYC obligations mean that intermediaries must know the names of their users, monitor their transactions and report activities that raise suspicions of money laundering or terrorist financing to the authorities. In addition to the law enforcement challenge, some developers are working to create crypto-assets that are particularly difficult to track, such as **Monero, Zcash and Dash**, which are known as *privacy coins*. These crypto-assets use hidden addresses and also create new addresses for each transaction. These types of conditions make it much easier for flows of illicit money to be hidden.

5.3.3. Mitigating the risks of laundering: towards a regulatory agenda of crypto-assets

The use of blockchain to validate and encrypt transactions with digital assets has been widely accepted, to the point that there are thousands of crypto-assets globally available. LIn 2021, New Zealand's financial authority estimated the existence **of more than 4,000**, while other sources document **over 6,000**. Although almost 90% of the total market could be concentrated in approximately 20 assets such as Bitcoin or Ethereum, the openness that characterizes the creation of these products makes it relatively easy to issue one.

The openness and decentralization underlying the mechanisms of crypto-asset creation and disintermediation in the DeFi ecosystem generates a variety of risks to the integrity of economic operations. Although they are beyond the scope of this study, they should be considered in regulating adoption of *blockchain*, in the issuance of crypto-assets, and in their use to carry out commercial or financial transactions. Digital currencies have been around for a decade; however, the regulatory systems that govern them are either highly fragmented or non-existent. This allows illicit activities ranging from fraudsters who "sell" Bitcoin and then disappear with the cash without exhausting the purchase, to terrorist financing and international money laundering to openly flourish (see table 5.2).

Table 5.2. Usage risks in crypto-assets and the DeFi ecosystem

Loss of confidence		Because they are not backed by a central bank, assets, a national or international organization, or other credit forms, crypto-assets are subject to a high degree of uncertainty. Moreover, their value is strictly determined by the value that market participants assign to them through their transactions. Consequently, a collapse of trading activities and a sharp drop in value can mean a great loss of confidence.
Cyber risk or fraud		Crypto-assets have attracted criminal networks. These criminals can break into crypto exchanges, drain crypto wallets and infect individual computers with crypto-asset stealing malware. As transactions are conducted over the Internet, hackers target individuals, service handlings and storage areas through means such as *phishing* and *malware*.
Compliance and regulation		Some countries may prevent the use of crypto-assets (as in the case of China, which banned the use of Bitcoin) or may claim that transactions violate anti-money laundering regulations. Due to the complexity, decentralized nature and the significant number of participants, including senders, receivers (possibly money launderers), processors (mining and trading platforms) and exchangers, there is no single approach to money laundering.
Market		There is a finite quantity of the currency, which means that it can suffer from liquidity problems, and limited ownership can make it susceptible to market manipulation. In addition, given its limited acceptance and lack of alternatives, the currency may appear more volatile, driven by speculative demand and exacerbated by hoarding.

The challenge for regulators is to find appropriate instruments to tackle the risks emanating from the increased adoption of crypto-assets (**Siwisa and Kern, 2021**). Existing regulatory instruments have limitations in addressing the risks of financial and consumer crime and of money laundering. For example, as a sign of progress on regulatory thinking the **Bank for International Settlements** (BPI)[88] declared crypto-assets to be speculative assets. It recommends authorities to first clarify regulatory classifications based on the

[89] Established in 1930, the BIS is owned by 63 central banks representing countries around the world. These 63 countries account for about 95% of the world's GDP. Its head office is located in Basel, Switzerland, and it has two representative offices in Hong Kong and Mexico City. From Latin America, the central banks of Argentina, Brazil, Chile, Colombia, Mexico and Peru are shareholders. The mission of the BIS is to "Support central banks' pursuit of monetary and financial stability through international cooperation and act as a bank for central banks" (see www.bis.org).

economic functions given to crypto-assets. Among other aspects, this shapes issues such as consumer protection (how to deal with property rights, theft and miss-selling); retail use (who can legitimately trade and under what conditions); treatment as securities (tradable instruments used to raise funds by representing a promise to pay in the future); and treatment as generic assets (i.e., tangible or intangible things that can be owned or controlled, e.g., houses).

In 2019, the Financial Action Task Force (FATF) introduced guidelines requesting governments to assess and mitigate; the risks associated with money laundering; and, the terrorist financing risks related to crypto-asset activities and service providers. It called for service providers to be registered and supervised by competent national authorities. However, the FATF reports that because only a quarter of the countries have adopted those guidelines and only some jurisdictions have anti-money laundering frameworks for using crypto-assets, criminals could quickly move to unregulated countries. The FATF encourages greater information sharing between countries regarding suspicious financial transactions involving crypto-assets, which is challenging, given that the anonymity of transactions needs to be eliminated. This last aspect is precisely what makes blockchain technology and encryption in private currencies so attractive.

5.4. Closing remarks and policy recommendations

Digital technologies are an invaluable ally that makes the fight against corruption more efficient when applied to integrity policies. AIn the context of the COVID-19 health emergency, Latin America faces unprecedented challenges; reducing poverty; social tensions and inequality; and promoting inclusive progress for all citizens. Curbing corruption is essential to achieve the development agenda's objectives because it protects public resources from undue interests and allows their efficient allocation for the provision of goods and services.

This way, incorporating digital innovations into public integrity policies requires adopting certain mechanisms within the technologies themselves. In other words, just as digital technologies are used for integrity, there is also an integrity agenda for those technologies and their applications. This agenda is considerable, particularly when taking into account that from the technological viewpoint alone, the platforms developed must have controls to verify the veracity of the data processed, or access and security protocols to approve sensitive operations through information systems, among other things.

In this section, there are three areas are of particular relevance that emphasize risk mitigation to safeguard integrity in the development of technologies, e.g., (i) digital identity fraud; (ii) the misuse of personal data; and (iii) the role of blockchain in the development and expansion of crypto-assets.

It is indispensable to adopt regulations that mitigate risks that were not previously prioritized, such as the creation of synthetic identities by digital means or the issuance of unregulated private digital currencies. Just as it would have been difficult for Gutenberg to see the potential of his printing press technology to drive the Protestant Reformation, today it is difficult for us to identify how digital acceleration will affect institutions such as the State or the Market Economy. Particularly, if the adoption of digital innovations for specific uses like the fight against corruption has consequences that differ from those originally conceived in their design. In this regard, some uses of technologies could be modified so that they do not pose risks to the integrity ecosystem.

- **Cyber or IT security is a major challenge and a vital component in the relationship of trust between citizens and government.** Cybersecurity capabilities are decisive when adopting any digital strategy. For this, risk and threat assessment are crucial, because once cybercriminals attack systems, their recovery requires large economic, human and time resources. Moreover, as risks may vary, these analyses must be carried out periodically.

It is essential to adopt regulations to mitigate risks that were not previously addressed. considered as a priority or relevant, such as the creation of synthetic identities by digital means or issuance of private currencies digital without any regulation.

- **Personal data can be captured by corruption networks within governments and by organized crime outside them.** Information ecosystems contain personal data, for which State agencies must ensure privacy and security. This implies planning, supervising and controlled data management. Likewise, an informed, risk-based approach with integrated privacy provisions is needed to trust digital identification systems.

- **International standards can serve as a model to create internal identity and access data management practices for individuals, according to their roles and with security access levels determined for different data categories.** They can also function to mitigate the risks of crimes related to identity theft and information tampering, and to help create full trust for citizens to interact online as their personal data will only be accessible to authorized entities and for authorized purposes.

- The following models can be mentioned as examples: the Resolution on Privacy in the Digital Age, adopted by the UN General Assembly in 2018; the 2013 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; the Proposed Declaration of Principles on Privacy and Personal Data Protection in the Americas adopted by the OAS Inter-American Juridical Committee in 2012 and 2015, respectively; the 2018 EU General Data Protection Regulation (GDPR); and, the 2020 California Consumer Privacy Act (CCPA).

- **As corruption networks find ways to move money and safeguard it from the rule of law, they thrive in an ecosystem interconnected by digital technology.** Cryptographic assets based on *blockchain* technologies mean that authorities would find it difficult to monitor, stop or reverse transactions occurring within these vast networks. Cross-border dialogue is imperative, especially between technology bureaus and authorities. The aim of this project is to develop financial intelligence systems to reduce money laundering risks on a transnational scale.

- **Regulation has been slow in responding to digital acceleration.** Although the potential benefits of *blockchain* help to increase regulatory efficiency by, for instance, adopting KYC policies (see chapter 4), this same technology allows transactions to be hidden in money laundering networks. In that sense, a consistent regulatory approach is required to align national criteria and enhance the role of regulation and supervision at the international level without restricting innovations required for the use of crypto-assets. To facilitate viable solutions and an informed debate on the regulation of *blockchain-based* digital financial assets, a close and continuous dialogue between the public and private sectors is also necessary.

6.

Public Policy Recommendations

Public Policy Recommendations

The digital acceleration experienced by the world today is disruptive in at least three aspects e.g., (i) the analysis of large datasets for predictive purposes on social phenomena is a reality[89]; (ii) such exercises require the concurrence of several disciplines around data science to fulfill their objective, and (iii) the predictive functionality of digital technologies is not their only virtue, it also allows them to act proactively and preventively against undesired acts of corruption.

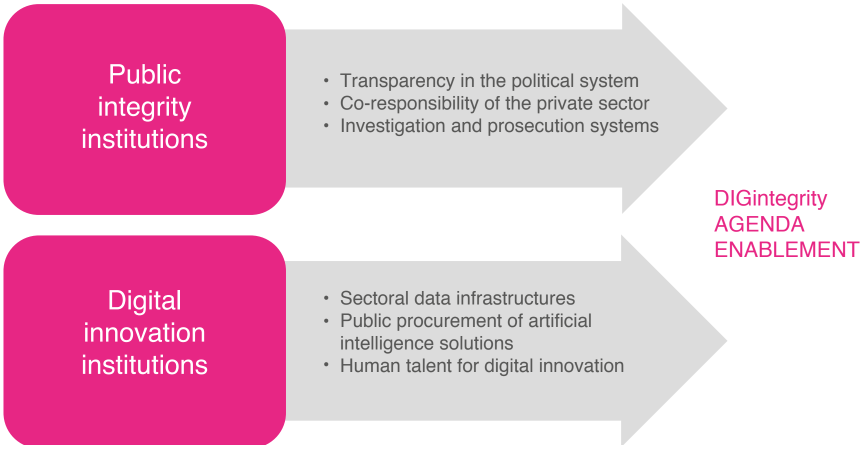
The role of data-driven technologies in public integrity is increasingly recognized by governments, multilateral organizations and civil society. Prevention and investigation of corruption can be faster and more effective due to the application of data science or technologies such as blockchain in public entities' management.

However, digital innovation; applying data-driven technologies; and, big data computing power are not silver bullets to eradicate corruption. Institutional contexts and governance frameworks that include aspects such as the relations between public sector and private enterprises, and between the State and society, are determinants for corruption networks to thrive or not (CAF, 2019). In an environment where the provision of public goods is exclusively defined by clientelist relationships, digital innovation could not contribute to eradicate corruption.

[89] This does not only apply to specific corruption phenomena, such as the improper signing of contracts or the diversion of public resources. Cetina (2021) provides examples of artificial intelligence platforms that seek to predict crime in urban areas or the violation of immigration laws. On the other hand, the industry of monetizing personal data (Zuboff, 2019) for targeted advertising purposes is based on predicting behaviors to consume information.

Exploiting digitalization's potential in public integrity policies involves adopting risk management policies to ensure integrity when using these technologies themselves and **moderating government institutions in two separate areas: institutional adjustments to promote integrity and public authorities' adaptability in the face of digitalization**. In this section of public policy recommendations, we address these areas for the effective implementation of digital innovations for public integrity.

Figure 6.1. Institutions for digital integrity and innovation.


Public integrity institutions
• Transparency in the political system
• Co-responsibility of the private sector
• Investigation and prosecution systems
DIGintegrity AGENDA ENABLEMENT
Digital innovation institutions
• Sectoral data infrastructures
• Public procurement of artificial intelligence solutions
• Human talent for digital innovation

6.1. Institutional adjustments for integrity in the digital era

Latin America faces immense challenges in advancing reforms that follow international standards on bribery prevention, conflict of interest and the abuse of public office to favor private interests (CAF, 2019; OECD, 2017). Coupled with the fact that data and information openness still require further development in the continent (Fumega, Scrollini and Zapata, 2021), these challenges, create considerable limitations for digital innovation to effectively prevent corruption.

Traditional approaches to the fight against corruption based on creating more punitive norms to punish crimes or misdemeanors have shown their limits. These should be complemented with preventive rules and institutions that regulate certain behaviors in the public service and promote private sector co-responsibility in anti-corruption policies. In this context, digitalization emerges as an additional alternative to facilitate private sector and civil society coordination within the public integrity agenda.

This report showed how citizens, oversight bodies, judicial authorities and executive branch entities can work together and cooperate through digital platforms to prevent corruption. Moreover, digital acceleration is changing the rules of the game in some processes related to formulating and implementing public policies such as tele-health, tele-education and remote justice. Therefore, it is important for the integrity agenda to also be attuned to these changes.

Latin America needs to modernize its institutional arrangements so its anti-corruption agenda is attuned to the digital acceleration and allows technologies to generate integrity dividends. Ensuring public service integrity presupposes regulations aimed at generating concrete standards of conduct. In the digital age, transparency standards and their enforcement can be massively recorded in data that makes integrity ecosystems more effective and efficient. This report selects three strategic groups of recommendations to advance institutional modernization and the DIGIntegrity agenda:

- **Political system transparency:** Igiven the need for funding to finance political campaigns, elections generate the first instances of State capture by corrupt agents, (CAF, 2019). The experience of major corruption cases in Latin America shows that illicit agreements were in fact gestated in the electoral phase.

- **Private sector co-responsibility:** private companies and civil society have strong incentives to influence public policy decisions. Moreover, they are important actors in electoral processes because they are able to finance political campaigns. Their co-responsibility in generating integrity in public policies and avoiding State capture should be part of the corruption fighting strategy.

- **Systems for legitimate, agile and restorative investigation and prosecution:** in Latin America, it is essential to enhance capacity to deter corrupt agents through a legitimate justice system that imposes effective sanctions. It is also essential to focus criminal and disciplinary procedures on the recovery of squandered or misappropriated resources and on reparations for corruption victims.

Political system transparency

Transparency in electoral processes is not restricted to counting and scrutinizing votes. Integrity in this area entails disclosing information on; the corporate structure of political campaigns; their income and expenditure; the identities of the natural and legal persons financing them; and, their suppliers.

- **Open records on different aspects of political financing should be subject to proactive transparency standards (as it occurs, for instance, with public procurement).** Open data on the activity of political parties and their movements during election time are necessary to transparentize electoral competition and to avoid the early capture of political activity by private interests (CAF, 2019).

- To find relationships and detect possible corruption networks between campaign financing and public procurement a network analysis, similar to the one carried out by the CGR in Colombia through DIARI, can be used to analyze political financing and public procurement. According to an analysis presented by the Electoral Observation Mission (MOE, by its acronym in Spanish), despite the existence of explicit legal prohibitions, political campaign donors receive multi-million contract adjudications after the election of financed candidates (MOE, 2018).

- **The digital era is also changing electoral processes thus requiring the design of integrity measures for the use of new technologies.** Progressively adopting electronic or remote voting poses integrity and transparency challenges in the counting and validation of votes. Particularly because digital identity must have robust authentication mechanisms.

- **Personal data protection policies should be articulated with the electoral campaigns' integrity in order** pto, for instance, avoid targeted

Practices using data and digital media to mobilize political campaigns should also be subjected to transparency measures and scrutiny and electoral oversight authorities.

advertising initiatives that use data originally collected for government purposes without citizens' consent. Practices using data and digital media to mobilize political campaigns should also be subject to transparency measures and scrutiny by citizens and electoral oversight authorities.

Private sector co-responsibility

Private interests are not harmful to public integrity by themselves; however, it is harmful to negotiate them while hiding in the shadows. Literature on the subject recognizes that public policies and problems are shaped in the political arena, the site where public and private interests converge (Dunn, 2018). Such concurrence is natural to democracy and the rule of law.

Following this internationally recognized principle, public integrity practices (OECD, 2017) require **disclosing private interests and drawing a punitive line with respect to the means used to negotiate interests**. For example, lobbying is accepted, but not bribery; similarly, private sector projects for Public-Private Partnerships (PPP) in infrastructure are also accepted, but not the revolving door to propose and execute them.

- **Latin America needs to advance in regulating public officials' conflicts of interest**[90] **by; developing legal frameworks; creating enforcement and conflict management bodies; and, establishing public registries of interests and asset declarations** (CAF, 2019; De Michele and Dassen, 2018). It is important for these registries to be in open data formats, updated annually and available for scrutiny and reuse by different institutions and citizens within the integrity ecosystem.

- **Moreover, lobbying requires a regulatory regime that allows a public registry containing lobbyist and clientele information, as well as the activities of natural or legal persons engaged in this activity** (CAF, 2019; OECD, 2021). Such data can be of great use for the integrity agenda. First, information openness allows scrutinizing public decision-making processes and the relationships between private sector and public officials. Second, that data can be deployed in preventive anti-corruption analytics.

- **Within the digital era's context, it is important for States to adopt open systems that generate trust in public decision-making.** EIn the process of approving laws, regulations or policies, organized disinformation schemes articulated through social networks can hinder public inter-

[90] In general terms, a conflict exists when a person's personal, occupational, economic or financial interests cannot be aligned with the functions of the office he/she holds. This happens because the personal interests could go against the general (or collective) interest that is protected by the performance of his or her official duties and responsibilities.

est and help position limited interest groups agendas (OECD, 2021). This generates pressure by combining organized presence in digital media and in political decision-making bodies. Moreover, this has the potential to completely exclude citizens affected by certain provisions from public discussions, and in so doing goes against the basic principles of democratic participation.

- **Finally, it is important to advance in the development of an official registry of final beneficiaries**[91]. CAF (2019) shows that Latin American governments show difficulties even in defining for legal purposes what constitutes a beneficial owner. Only 5 out of 26 countries have a clear definition of the concept that conforms to FATF standards against money laundering. Capture of State management by private interests becomes more feasible when individuals find ways to hide behind corporate vehicles in order to contract with governments, influence public decisions and even

[91] Natural persons who are the true owners or controllers, or who benefit economically from a legal vehicle, such as a commercial company, a trust, a foundation, etc.

deliberately engage in crimes such as money laundering. Having beneficial ownership registries would help governments prevent money laundering-related crimes, enforce tax compliance and increase tax collection.

Investigation and prosecution systems

The processes of investigating and sanctioning corruption can be streamlined with digital technologies, that allow collecting, analyzing and presenting data on the risks and structures behind corruption in a quick and intuitive way and without losing relevant information (see chapter 3). However, this potential may be lost if judicial or administrative processes are slow or complicated throughout their distinct stages, or, when legal institutions are manipulated by the accused in order to circumvent investigation and prosecution systems. Even though in the last two decades criminal procedure in Latin America was reformed to make justice more efficient, these measures are more useful in solving cases of flagrancy or others, where collaboration agreements with the authorities can be achieved quickly (CAF, 2019).

On the other hand, corruption offenses require coordinated technical work involving several authorities which slows down the procedures, as they go through certain evidence gathering protocols to indict before judges. PFor instance, forfeiture of ownership of illicitly acquired assets requires a great amount of coordination between judges, prosecutors, judicial police and other competent authorities to successfully complete the procedure —even when authorities have information and data on the assets to be seized. If protocols are complicated and time consuming then the accused can easily become insolvent[92], Ithe justice system can lose its deterrence capacity, and resources or economic means to repair the victims, even in the case of State entities, are squandered.

It is necessary to strengthen the upskilling and retention of talent that can effectively use digital technologies in the exercise of functions such as corruption prevention, investigation and detection.

Digitalization by itself does not make procedures simpler or more efficient (Roseth et al., 2018), neither does it make investigating or prosecuting corruption more effective. In this regard, the recommendations are:

- **Simplify investigative procedures and processes, and strengthen special anti-corruption agencies to ensure the effectiveness of prosecutions against corrupt actors.** LTo effectively combat this complex and changing occurrence, the terms of investigation, resources and tools available to judicial, administrative authorities and control agencies must be sufficiently robust.

[92] This, in the digital era, would happen, paradoxically, due to the technologies that the Government itself enables to streamline notarial procedures, real estate purchases and sales, financial asset transfers and transactions in the FinTech environment, to cite just a few examples.

- **Strengthen and promote coordination between judicial authorities and control agencies in charge of the anti-corruption agenda**. A single corrupt conduct may open room for different prosecutions and liability regimes for the State and private agents involved. Joint work is crucial to avoid effort duplications, delays in proceedings, impunity and contradictory decisions regarding corrupt actors.

- **One thing that could contribute to making justice more expeditious and dissuasive are compensated confessions** (CAF, 2019). The negotiation of penalties in exchange for the accused's confession and information about the criminal networks they belong to are an invaluable ally for the justice system to apply sanctions and dismantle the structures behind corruption. It is key for negotiations of this kind to also include the provision of property information, corporate vehicles and other illicitly acquired assets. This way, justice becomes both dissuasive and restorative: it reduces the potential economic benefit for the corrupt and also collects assets to repair victims of corruption.

6.2. Institutional adjustments for digital innovation in governments

Institutions in charge of anti-corruption policy must buy or develop digital solutions to facilitate their work or make it more effective. They must also foster an environment that allows the generation of innovative solutions to prevent, investigate and detect corruption. Just as the locomotive required railroads for its performance and to contribute to the Industrial Revolution, governments in general, and anti-corruption institutions in particular, need to adjust some aspects of their innovation environment before implementing digital technologies for integrity.

In this regard, at the very least, the following conditions are required to facilitate the adoption of digital innovation practices for public integrity strategies:

- **Organized data infrastructures for each sector of public management.** PSince corrupt agents have different strategies and approaches to the different types of public goods provided by the State (health, education, security, justice, infrastructure, etc.), sector-specific datasets increase the effectiveness of digital technologies for integrity.

- **Digital talent in agencies responsible for anti-corruption policy.** The incorporation of digital technologies in public integrity strategies, takes the knowledge and expertise of those who handle and manage them for granted. This is not always the case with public officials in Latin America. Therefore, it is necessary to strengthen the upskilling and retention of talent that can effectively use digital technologies in the exercise of functions such as corruption prevention, investigation and detection. **Creating units specialized in data science and intelligence within control agencies can help solve digital gaps related to human talent in the integrity ecosystem.**

- **Public procurement of artificial intelligence.** Just as there are special standards to ensure integrity and quality in public procurement of infrastructure (Fajardo *et al.*, 2021), it is equally strategic for public entities to develop standards to structure needs and processes to source artificial intelligence platforms with anti-corruption purposes. There are ethical and accountability standards for this technology that influence its use and quality. Additionally, digital innovations aimed at improving transparency levels can be shared and reused through open source by other public entities or CSOs interested in the fight against corruption.

Sectoral data infrastructures

In Latin America, significant challenges persist in terms of the quality, usability and sustainability of government open data initiatives related to public integrity and corruption prevention. With the advent of the pandemic, the need for the capacity to implement data policies that protect public interest became tangible. **In particular, the urgency of adopting data infrastructure practices on the following fronts has become evident**:

- **To manage open data, it is necessary to enable data linkage and interoperability through appropriate management systems.** Interoperability relates to the use of standards to represent data. This in turn means that related data can be easily brought together. Linkage relates to the use of standard identifiers within datasets, allowing records to connect to additional data from another set (Coyle, Kay, Diepeveen, Tennison, & Wdowin, 2020).

- **Corruption is sectoral and specific; therefore, it is necessary to improve relevant data for the prevention of corruption in those sectors.** In terms of integrity, the most strategic datasets have already been defined through initiatives such as the Inter-American Open Data Program (PIDA, by its Spanish acronym) (see chapter 1). However, we must bear in mind that corruption also has a sectoral dimension (Campos and Pradhan, 2007). That is, there are subtle variations in the commission of crimes or in the capture of public institutions and resources that depend on the sector that corruption aims to plunder. It may be that the capture of resources in infrastructure is more lucrative through the public procurement of large projects (CAF, 2019), but in the health sector, criminals may find it more lucrative to extract resources by committing fraud in insured beneficiary records and billed services.

Consequently, in order to properly identify corruption in each sector and to improve the quality of public administration's decision making, it is important for governments to define specific data infrastructures for public management sectors. It may be that in the infrastructure and public works sector investment project data and their accompanying contracts are extremely important in terms of integrity. However, in the health sector, the quality of data on reimbursements for services rendered in the insurance system requires refinement.

It is necessary for governments to adopt mechanisms for regional and international dialogue and cooperation in order to ensure a uniform data structure.

Coordinated responses must also be strengthened through better interoperability between government agencies and countries. This would enable more accurate decision-making to attack corruption networks at the global, national and local level. To this end, to properly ensure a uniform data structure governments must adopt mechanisms for regional and international dialogue and cooperation. Likewise, operational cooperation allows experiences (platforms, applications, systems) to be shared in an open-source format which facilitates the exchange of information, action updates and results discussions. This cooperation has been promoted among the region's comptrollers' offices through the Latin American and Caribbean Organization of Supreme Audit Institutions (OLACEFS, by its Spanish acronym) and the International Organization of Supreme Audit Institutions (INTOSAI, by its acronym in Spanish).

Public procurement of artificial intelligence

Digital solutions that use AI to process data face an inherent fallibility, which can be best summarized in Moravec's paradox[93]. Consequently, in AI development, investment in computing power resources focuses on those simple cognitive aspects that, if not considered, could lead to inaccurate and biased results (Cetina, 2021). The application of IA solutions by governments may yield inaccurate recommendations or predictions, due to this technology's fallibility. Additionally, AI solutions may conflict with the fundamental rights of the citizens who are affected by the automated decisions of these platforms (CAF, 2021; Cetina, 2021).

In general, in public procurement processes, any government strategy based on AI should take into account the following recommendations.

- **Responsible public procurement of AI technologies begins with proper structuring and planning which contemplates a compulsory framework to supply data governance contracts.** Governments may find it more convenient not to take charge of developing AI solutions to prevent corruption by themselves or in-house and instead procure them or ask private parties to develop them.

- **Frameworks that regulate public procurement of artificial intelligence (CPIA, by its Spanish acronym) should include transparency and common reference terms for procurement, design, development and use of AI-based systems.** Just as in large bidding processes for public works or for high-impact public projects, the State's use of artificial intelligence systems must abide by open procurement standards. That way, all relevant stakeholders are invited to provide input, comments and exercise social control over public procurement processes ranging from the structuring of reference terms to the final delivery of the contracted goods through a multidisciplinary approach (Council of Europe, 2019).

[93] Informally stated, the paradox proposes that it is very easy for computers to perform reasoning tasks that humans find very complicated (for example, calculating the natural logarithm of 1,357); while cognitive tasks that are simple for humans (such as recognizing a human face) are very difficult for a computer.

- **CPIA's planning and execution must ensure the participation of those who have contributed to data generation or are affected by the algorithm's decisions.** In the case of the fight against corruption, this development will imply the adoption of mechanisms for dialogue between the judicial branch, financial intelligence, the executive branch and control agencies.

- **Mechanisms for security, reliability, transparency and explainability should be incorporated. Ethical principles should also be adopted to structure public procurement of AI solutions (CAF, 2021).** Moreover, there should be accountability processes and ongoing evaluations of digital platforms and technologies that manage data with AI technologies. This should include measures that guarantee a traceability that documents the methods used to train the produced algorithms. Likewise, governments should clearly communicate the characteristics, limitations and possible deficiencies of the AI system.

Human talent for the digital era

- **Digital innovations and data reuse techniques to improve public integrity entail rethinking the skills required by officials in institutions related to the prevention, detection, investigation and punishment of corruption.** Successfully driving this process implies having digital specialists within the cast of public servants.

- This is not restricted to hiring programmers. **It also requires promoting the concurrence and interaction of multidisciplinary teams composed by; lawyers; data scientists; auditors and engineers; among others, that learn to reuse data and adopt digital technologies in the exercise of their functions.** According to Ripani and Roseth (2021), Latin America faces great challenges in this area: 51% of public officials acknowledge having a severe or very severe deficit of data analysis skills in their teams.

- In this regard, CAF (2021) proposes that **public institutions adopt strategies to develop human resources, starting with a measurement of public employee's readiness to use and embrace digital technologies**. After this measurement it is necessary to adopt an upskilling plan to be implemented within the framework of a management change process.

- **In the integrity ecosystem in particular, this type of plan should be oriented to developing a workforce with the required profiles and skills and who can articulate uses for digital technologies in line with the administrative procedures of prevention and surveillance.** To this end, it is necessary to have the skills to permanently adapt to expected changes in the nature of the tasks to be implemented, and to perform satisfactorily in new environments. This entails developing soft skills (socio-personal skills) and hard skills (specialized or technical skills).

Agencies responsible for investigating and controlling corrupt activities should have offices or units specialized in data science and intelligence.

- Rather than requesting folders and documents to verify compliance with seals, signatures and procedures **public procurement auditors, in particular, must know how to consult data from public procurement portals and rely on them to identify networks and patterns.** For instance, this also means learning and using new concepts, such as digital signatures or authentication by digital means (see chapter 5), which gradually but surely simplify bureaucratic processes.

- **Agencies responsible for investigating and controlling corrupt activities should have offices or units specialized in data science and intelligence.** In 2020, Colombia's Office of the Inspector General created the Information and Intelligence Management Unit. Among its functions is to design and implement instruments that provide the information necessary to identify and address corruption risks and mismanagement. In Peru, in 2021, the Data Analysis Deputy Management was created as part of the internal restructuring of the Office of the Comptroller General of the Republic. Among other tasks, it identifies corruption risks and acts in the use of public resources and formulates policies and strategies to store and process information.

- **In the anti-corruption agenda's framework, international institutions can promote the exchange of experiences and good practices in the development of digital innovations.** Organizations such as OLACEFS and INTOSAI foster cooperation among control bodies in Latin America. Thanks to the digital revolution, these alliances can be expanded globally.

REFERENCES

Aarvik, P. (2020). Blockchain as an anti-corruption tool. Case examples and introduction to the technology. *U4 Issue, 2020:7*. **https://www.cmi.no/publications/7208-blockchain-as-an-anti-corruption-tool-case-examples-and-introduction-to-the-technology**

Agencia EFE. (2020). Investigan un presunto hackeo de la división digital del Gobierno de Chile. **https://www.efe.com/efe/america/economia/investigan-un-presunto-hackeo-de-la-division-digital-del-gobierno-chile/20000011-4368087**

Agudelo, M. (2021). La economía y las industrias digitales basadas en el conocimiento. *Documentos de políticas para el desarrollo*, n.º 8. **https://scioteca.caf. com/handle/123456789/1766**

Aliyev, Z. y Safarov, I. (2019). *Logos, mythos and ethos of blockchain: An integrated framework for anti-corruption.* OECD Global Anti-Corruption & Integrity Forum.

Almeyda, N. (2020) Criptomonedas vs. criptoactivos: un problema de identidad con repercusiones jurídicas. Universidad Externado de Colombia. Tesis de Maestría en Derecho Económico con énfasis en Teoría del Derecho Económico y la Regulación. Recuperado de: **https://bdigital.uexternado.edu.co/bitstream/handle/001/3591/GEADA-spa-2020 Criptomonedas_vs_criptoactivos_un_problema_de_identidad_con_repercusiones_juridicas?sequence=1&isAllowed=y**

Andersen T. B.; Bentzen, J.; Dalgaard, C-J. y Selaya, P. (2011). Does the Internet Reduce Corruption? Evidence From U.S. States and Across Countries. World Bank Economic Review. 25(3): pp. 387-417.

Arbache, J. (2020). ¿Bancos o fintechs? CAF. Recuperado de: **https://www.caf.com/es/conocimiento/visiones/2020/12/bancos-o-fintechs/**

Ash, E.; Galletta, S. y Giommoni, T. (2020). *A Machine Learning Approach to Analyze and Support Anti-Corruption Policy.* WP Series ETH Zurich Center for Law & Economics.

Atencio, J. M. (2019). Los contratos inteligentes (*smart contracts*). En: Contract management/ compilado por Ricardo Antonio Parada; José Daniel Errecaborde. – 1.ª ed. - Ciudad Autónoma de Buenos Aires. Erreius. Errepar.

Atencio, J. M. (2020). Contratación pública y futuro: pensando en el *blockchain*. En: Temas de Derecho Administrativo – Erreius – Errepar.

Banco Mundial (2013). El registro de nacimientos: La llave para la inclusión social en América Latina y el Caribe. **https://publications.iadb.org/es/publicacion/14834/el-registro-de-nacimientos-la-llave-para-la-inclusion-social-en-america-latina-y**

Banco Mundial (2014). Digital Identity Toolkit. A guide for stakeholders in Africa. World Bank. **https://openknowledge.worldbank.org/bitstream/handle/10986/20752/912490WP0Digit00Box385330B00PUBLIC0.pdf?sequence=1&isAllowed=y**

Banco Mundial (2019). ID4D Practitioner's Guide (English). Identification for Development Washington, D.C.: World Bank Group. Recuperado de: **http://documents.worldbank.org/curated/en/248371559325561562/ID4D-Practitioner-s-Guide**

Banco Mundial (2021). Global Identification Challenges by the Numbers. 2018 estimates. Recuperado de: **https://id4d.worldbank.org/global-dataset/visualization**

Bailard, C. S. (2009). Mobile phone diffusion and corruption in Africa. *Political Communication,* 26(3), pp. 333-353.

Banerjee, A.; Duflo, E.; Imbert, C.; Mathew, S. y Pande, R. (2020). E-governance, accountability, and leakage in public programs: Experimental evidence from a financial management reform in India. *American Economic Journal. Applied Economics,* 12(4), pp. 39-72.

Becker, G. S. y Stigler, G. J. (1974). Law enforcement, malfeasance, and compensation of enforcers. *The Journal of Legal Studies,* 3(1), pp. 1-18.

Beduschi, A. (2021). Rethinking digital identity for post-COVID-19 societies: Data privacy and human rights considerations. Data & Policy, 3, E15. **doi:10.1017/dap.2021.15**

BIS. (2001). *Customer Due Diligence for Banks, Basel Committee on Banking Supervision* (Bank for International Settlements). **http://www.bis.org/publ/bcbs77.pdf**

BIS. (2018). *BIS Annual Economic Report. V. Cryptocurrencies: Looking beyond the hype* (pp. 91-113).

Bjorkman, M. y Svensson, J. (2009). Power to the People: Evidence from a Randomized Field Experiment on Community-Based Monitoring in Uganda. *Quarterly Journal of Economics*, 124(2), pp. 735769.

Blockchain technology to prevent corruption in Covid-19 response: How can it help overcome risks? (s. f.). Cmi.No. Recuperado de: **https://www.cmi.no/publications/7259-blockchain-technology-to-prevent-corruption-in-covid-19-response-how-can-it-help-overcome-risks** (consulta realizada el 22 de octubre de 2021).

Blockchain, O. (s. f.). *OECD Blockchain Primer.* Secretary-General of the OECD. Recuperado de: **https://www.oecd.org/finance/OECD-Blockchain-Primer.pdf** (consulta realizada el 9 de octubre de 2021).

Bojanic, D. y Madsen, E. (2014). *The Effect of Internet and Digital Media Freedom in Corruption*. **http://pure.au.dk/portal-asb-student/files/79187961/The_Effect_of_Internet_and_Digital_Media_Freedom_on_Corruption.pdf**

Bologna, J. (2014). Is the Internet an effective mechanism for reducing corruption experience? Evidence from a cross-section of countries. *Applied Economics Letters*, 21(10), pp. 687-691.

Bott, J. y Milkau, U. (2017). Central bank money and blockchain: A payments perspective. *Journal of Payments Strategy & Systems*, 11(2), pp. 145-157.

Brugués, F.; Brugués, J. y Giambra, S. (2018). *Political connections and misallocation of procurement contracts: Evidence from Ecuador*. **http://scioteca.caf.com/handle/123456789/1394**

CAF. (2019). RED 2019. Integridad en las políticas públicas: claves para prevenir la corrupción. Recuperado de: **http://scioteca.caf.com/handle/123456789/1503**

CAF. (2021a). *CAF promueve la transparencia y la rendición de cuentas en proyectos de infraestructura de Latinoamérica*. Caf.Com. **https://www.caf.com/es/actualidad/noticias/2021/05/caf-promueve-la-transparencia-y-la-rendicion-de-cuentas-en-proyectos-de-infraestructura-de-latinoamerica/**

CAF. (2021b) ExperiencIA: Datos e Inteligencia Artificial en el sector público. Recuperado de: **https://scioteca.caf.com/handle/123456789/1793**

Campos, J. y Pradhan, S. (2007). The Many Faces of Corruption: Tracking Vulnerabilities at the Sector Level. Washington, DC: World Bank. **https://openknowledge.worldbank.org/handle/10986/6848 License: CC BY 3.0 IGO.**

Cardona, D.; Cortés, J. y Wong, M. (2015). Diagnóstico de transparencia en municipios de Panamá. Estudio de caso de la segunda fase del programa de gobierno electrónico de la Organización de los Estados Americanos: municipios eficientes y transparentes. MuNet. *UPIICSA Investigación Interdisciplinaria*, 1(2), pp. 1-31.

Carvalho, R.; Marzagao, T.; Paula, E. y Ladeira, M. (2017). Deep Learning Anomaly Detection as Support Fraud Investigation in Brazilian Exports and Anti-Money Laundering. *15th IEEE International Conference on Machine Learning and Applications (ICMLA)*.

Castellón, P. y Velásquez, J. (2013). Characterization and Detection of Taxpayers with False Invoices using Data Mining Techniques. *Expert Systems and Applications*, 40(5), pp. 1427-1436.

Cetina, C. (2020a). *Blockchain e integridad: aplicaciones de política pública*. Caf.Com; CAF. **https://scioteca.caf.com/handle/123456789/1651**

Cetina, C. (2020b). *Tecnología para la integridad en tiempos del COVID-19*. Caf.Com; CAF. **https://scioteca.caf.com/handle/123456789/1542**

Cetina, C. (2020c). *Tres preguntas sobre el uso de los datos para luchar contra la corrupción.* Caf.Com; CAF. **https://scioteca.caf.com/handle/123456789/1544**

Cetina, C. (2021a). *Gobernanza de datos y capacidades estatales para la pospandemia.* Caf. Com; CAF. **https://scioteca.caf.com/handle/123456789/1765**

Cetina, C. (2021b). La aceleración digital de los Gobiernos e implicaciones de política pública. *Documentos de Políticas para el Desarrollo*, n.º 16. **https://scioteca.caf.com/handle/123456789/1782**

Cetina, C., Fonseca, H. y Zuleta, M. (2021). Diagnóstico subregional de los datos del sistema de compra y contratación pública. Organización de los Estados Americanos (OEA) y el Banco de Desarrollo de América Latina (CAF). **http://ricg.org/wp-content/uploads/2021/05/Diagnostico-subregional-de-los-datos-del-sistema-de-compra-y-contratacion-publica.pdf**

Cetina, C., Garay Salamanca, L. J., Salcedo-Albarán, E., y Vanegas, S. (2021). La analítica de redes como herramienta de integridad: el caso de la Procuraduría General de la Nación en Colombia. Caracas: CAF. Recuperado de: **http://scioteca.caf.com/handle/123456789/1675**

Chainalysis. (2021). The Chainalysis 2021 Crypto Crime Report.

Chêne, M. (2012). *Impact of community monitoring on corruption. U4 Anti-Corruption Resource.*

Chiesi, A. M. (2001). Network Analysis, Editor(s): Neil J. Smelser, Paul B. Baltes, *International Encyclopedia of the Social & Behavioral Sciences, Pergamon,* 2001, pp. 10499-10502, **https://doi.org/10.1016/B0-08-043076-7/04211-X**

Choi, J. W. (2014). E-Government and Corruption: A Cross-Country Survey. *World Political Science,* 10(2), pp. 217-236.

CIAT (2018) BLOCKCHAIN: Concepts and potential applications in the tax area. **https://www.ciat.org/blockchain-concepts-and-potential-applications-in-the-tax-area-13/?lang=en**

Consejo Europeo. (2020). Digital Solutions To Fight Covid-19. Data Protection Report. **https://rm.coe.int/prems-120820-gbr-2051-digital-solutions-to-fight-covid-19-text-a4-web-/16809fe49c**

Cong, L. W. y He, Z. (2018). *Blockchain Disruption and Smart Contracts.* National Bureau of Economic Research.

Cordova, Y. y Gonçalves, E. (2019) Rosie the Robot: Social accountability one tweet at a time. Banco Mundial. **https://blogs.worldbank.org/governance/rosie-robot-social-accountability-one-tweet-time**

Cormen, T.; Leiserson, C.; Rivest, R. y Stein, C. (2001). Introduction to Algorithms (Segunda edición). MIT Press and McGraw-Hill

Corredor, O. (2018). *El PAE y la inasistencia escolar: el rol del tipo de contratación y la capacidad institucional del municipio*. Universidad del Rosario.

Coyle, D.; Kay, L.; Diepeveen, S.; Tennison, J. y Wdowin. J. (2020). The value of data - Policy Implications. Bennett Institute, University of Cambridge Open Data Institute. **https://www.bennettinstitute.cam.ac.uk/publications/value-data-policy-implications/**

Cruz, G. (2020). *GovTech y el futuro del Gobierno: el caso de Datasketch en Colombia.* Caf. Com; CAF. **https://scioteca.caf.com/handle/123456789/1539**

Csonka, P. (2006). The Council of Europe's Convention on Cybercrime and Other European Initiatives. *Revue Internationale de Droit Pénal, 77*(3), 473.

Datos Abiertos ChileCompra. (2021). Chilecompra.Cl. **http://datosabiertos.chilecompra.cl**

Datos básicos: La lucha contra la corrupción. (2021). Bancomundial.Org. **https://www.bancomundial.org/es/news/factsheet/2020/02/19/anticorruption-fact-sheet**

Davis, M.; Lennerfors, T.T. y Tolstoy, D. (2021). "Can blockchain-technology fight corruption in MNEs' operations in emerging markets?", *Review of International Business and Strategy*, Vol. ahead-of-print No. ahead-of-print. **https://doi.org/10.1108/RIBS-12-2020-0155**

De Michele, R. y Dassen, N. (2018). Conflicto de intereses: Desafíos y oportunidades para implementar un sistema efectivo de prevención y control. BID. **http://dx.doi.org/10.18235/0001362**

De Michele, R. y Pierri, G. (2020). *Transparencia y gobierno digital: El impacto de COMPR.AR en Argentina*. BID. **http://dx.doi.org/10.18235/0002335**

De Roux, D.; Pérez, B.; Moreno, A.; Villamil, M. y Figueroa, C. (2018). Tax Fraud Detections Using and Unsupervised Machine Learning Approach. *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining KDD '18.*

Deloitte. (2019). *Data governance has always been important, and a changing risk and regulatory landscape is accelerating the need for a strong, strategic program*. Deloitte. Com. **https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-rfa-data-governance-program-tmt-companies.pdf**

Development Matters. (5 de agosto de 2021). *La digitalización como estrategia anticorrupción.*

Oecd-Development-Matters.Org. **https://oecd-development-matters.org/2021/08/05/la-digitalizacion-como-estrategia-anticorrupcion/**

Digiampietri, L.; Trevisan, N.; Meira, L.; Jambiero, J.; Ferreira, C. y Kondo, A. (2008). *Uses of Artificial Intelligence in the Brazilian Customs Fraud Detection System*.

Digital Denmark – Experience Denmark's digitization. (s. f.). Digitaldenmark.Dk. Recuperado de: https://digitaldenmark.dk (consulta realizada el 22 de octubre de 2021).

Does the Internet reduce corruption? Evidence from US states and across countries. (2011). *The World Bank Economic Review.*

Domínguez, G. y Gerbasi, N. (2020). *Govtech y el futuro del gobierno: el ecosistema govtech en Brasil. Nuevas tecnologías y nuevas alianzas público-privadas para mejorar los servicios públicos*. **http://scioteca.caf.com/handle/123456789/1582**

Editorial La República S. A. S. (s. f.). *Delito de suplantación de identidad aumentó 409 % en 2020 debido a la pandemia.* Com.Co. Recuperado de: **https://www.asuntoslegales.com.co/actualidad/delito-de-suplantacion-de-identidad-aumento-409-en-2020-debido-a-la-pandemia-3151651** (consulta realizada el 22 de octubre de 2021).

e-Estonia — We have built a digital society and we can show you how. (Diciembre 10 de 2019). E-Estonia.Com. **https://e-estonia.com**

English, M.; Auer, S. y Domingue, J. (2015). *Block Chain Technologies & The Semantic Web : A Framework for Symbiotic Development.*

ESIP. (2018). *"E-SOCIAL SECURITY: ANTICIPATING THE FUTURE*. Esip.Eu. **https://esip.eu/images/pdf_docs/Scoping-paper-Workshop-1-Digital-tools-for-information-exchange.pdf**

Exploring blockchain technology for government transparency: Blockchain-based public procurement to reduce corruption. (s. f.). Weforum.Org. Recuperado de: **https://www.weforum.org/reports/exploring-blockchain-technology-for-government-transparency-to-reduce-corruption** (consulta realizada el 22 de octubre de 2021).

Fajardo, G.; López, M.; Ramírez, A.; Román, C.; Silveira, A. y Zarama, D. (2021). *Gobernanza del sector de infraestructura y de las APP.* CAF. **https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html**

Fazekas, M. y Kocsis, G. (2020). Uncovering High-Level Corruption: Cross-National Objective Corruption Risk Indicators Using Public Procurement Data. British Journal of Political Science, 50(1), 155–164. **https://doi.org/10.1017/S0007123417000461**

Few, S. (2014). Data Visualization for Human Perception. En: The Encyclopedia of Human-Computer Interaction, 2nd Ed. INTERACTION DESIGN FOUNDATION.

FDA. (2020). *Blockchain Interoperability Pilot Project Report.* **https://www.merck.com/wp-content/uploads/sites/5/2020/07/FDA_DSCSA_Interoperability_Pilot_Project-Final_Report_Feb2020.pdf**

Fidler, B. (2017). Cybersecurity Governance: A Prehistory and its Implications. *Digital Policy Regulation and Governance*, 19(6), pp. 449-465.

FINRA. (2019). Know Your Customer. Finra.Org. **https://www.finra.org/rules-guidance/rulebooks/finra-rules/2090**

Freire, D.; Galdino, M. y Mignozzetti, U. (2020). Bottom-Up Accountability and Public Service Provision: Evidence from a Field Experiment in Brazil. Research and Politics, 7(2).

Fuente, G. (2014). El derecho de acceso a la información pública en América Latina y los países de la RTA: Avances y desafíos de la política. *En Transparencia & Sociedad.* Edición 2. **https://archives.cplt.cl/artic/20140701/asocfile/20140701161427/t_s_n2web.pdf**

Garay, L. G.; Salcedo-Albarán, E. y Macías, G. (2018) Macrocorrupción y cooptación institucional: la red criminal "Lava Jato"

Garay, L. G.; Salcedo-Albarán, E. y Macías, G. (2021). Súper-red de corrupción en Venezuela.

Gallego, J. (2021). *Evidencia cuantitativa sobre el efecto de las iniciativas de gobierno digital en el fenómeno de la corrupción.*

Gallego, J.; Maldonado, S. y Trujillo, L. (2020). From Curse to Blessing: Institutional Reform and Resource Booms in Colombia. *Journal of Economic Behavior & Organization*, 178, pp. 174-193.

Gallego, J.; Rivero, G. y Martínez, J. (2021). Preventing rather than Punishing: An Early Warning System of Malfeasance in Public Procurement. *International Journal of Forecasting*, 37(1), pp. 360-377.

Gelb, A. y Clark, J. (2013). "Identification for Development: The Biometrics Revolution". Working Paper 315, Center for Global Development, Washington, DC.

Gigler, S. y Bailur, S. (2014). Closing the Feedback Loop: Can Technology Bridge the Accountability Gap? *Directions in Development--Public Sector Governance*;. Washington, DC: World Bank. https://openknowledge.worldbank.org/handle/10986/18408

Goede, M. (2019). E-Estonia: The E-Government Cases of Estonia, Singapore, and Curaçao. *Archives of Business Research*, 7(2). https://doi.org/10.14738/abr.72.6174

González, V. (s. f.). MuniDigital wants to be the "Spotify" of the Smart Cities. The Smartcity Journal. Recuperado de: https://www.thesmartcityjournal.com/en/sustainability/munidigital-wants-to-be-the-spotify-of-the-smart-cities

Grace, E.; Rai, A.; Redmiles, E. y Ghani, R. "Detecting fraud, corruption, and collusion in international development contracts: The design of a proof-of-concept automated system", 2016. IEEE International Conference on Big Data, Washington, DC, 2016, pp. 1444-1453.

Graglia, J. M. y Mellon, C. (2018). Blockchain and Property in 2018: At the End of the Beginning. *Innovations Technology Governance Globalization*, 12(1–2), pp. 90-116.

Granados, R. y Rodríguez, J. (2013). *Publicidad y transparencia en la actividad contractual de las administraciones públicas.*

Haafst, R. (2017). *On The Effect of Digital Transformation on Corruption: An inter-country analysis.* Unpublished. https://doi.org/10.13140/RG.2.2.10163.43044

Haber, S. y Stornetta, W. S. (1991). How to Time-Stamp a digital document. *Journal of Cryptology* 3, pp. 99-111. https://doi.org/10.1007/

Heller, N. (2017). *Estonia, the Digital Republic.*

Houlder, V. (2017). Ten ways HMRC can tell if you're a tax cheat. En: Financial Times. Diciembre 2017. https://www.ft.com/content/0640f6ac-5ce9-11e7-9bc8-8055f264aa8b

ID4D Practitioner's Guide (English). Identification for Development Washington, *D.C. (2019). Worldbank.Org.* http://documents.worldbank.org/curated/en/248371559325561562/ID4D-Practitioner-s-Guide

ILDA. (2020). *Barómetro Regional de Datos Abiertos para América Latina y el Caribe 2020.* https://barometrolac.org/wp-content/themes/odbpress/reporte-ILDA-ES.pdf

Insurance Information Institute. (s. f.). *Facts + Statistics: Identity Theft and Cybercrime*. Iii.Org. Recuperado de: https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (consulta realizada el 22 de octubre de 2021).

International Monetary Fund. Legal Dept. (2018). Colombia: Financial Sector Assessment Program – Detailed Assessment Report on Anti-Money Laundering and Combating the Financing of Terrorism. *IMF Staff Country Reports,* 18(314), p. 1.

Interpol. (2020). *Shift in targets from individuals to governments and critical health infrastructure*. https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

Irwin, L. (2021). *Personal data vs. sensitive data: what's the difference?* https://www.itgovernance.co.uk/blog/the-gdpr-do-you-know-the-difference-between-personal-data-and-sensitive-data

Keefer, P. y Roseth, B. (2021). *Grand Corruption in the Contracting Out of Public Services: Lessons from a Pilot Study in Colombia*. IDB Working Paper Series.

Kelsen, H. (1949). *Teoría General del Derecho y del Estado*. Harvard University Press.

Kelsen, H. (2017). *General theory of law & state* (Hans Kelsen & A. J. Treviño, Eds.). Routledge.

Ko, T.; Lee, J. y Ryu, D. *Blockchain Technology and Manufacturing Industry: Real-Time Transparency and Cost Savings,* 10 Sustainability (Basel, Switzerland) 4274 (2018), available at **https://search.datacite.org/works/10.3390/su10114274.**

Koch, R. (2019, February 1). *What is considered personal data under the EU GDPR?* Gdpr.Eu. **https://gdpr.eu/eu-gdpr-personal-data/**

Kofax. (2020). *Global E-Signature Law: Best Practices for Assessing Risk.* **https://ordiginal.com/wp-content/uploads/2020/10/eb_global-e-signature-law_en.pdf**

KPMG. (2016). *New Electronic Tax Payment System Requirements.* **https://assets.kpmg/content/dam/kpmg/pdf/2016/06/id-kai-tax-news-flash-january-2016-electronic-tax-payment.pdf**

Laajaj, R.; Eslava, M. y Kinda, T. (2019). The costs of bureaucracy and corruption at customs: Evidence from the computerization of imports in Colombia. *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.3334529

Latin American Countries Encouraged to use KYC processes. (19 de marzo de 2019). *AU10TIX*. **https://www.au10tix.com/BLOG/LATIN-AMERICAN-COUNTRIES-ENCOURAGED-TO-USE-KYC-PROCESSES/**

Lauletta, M.; Rossi, M.; Cruz, J. y Arisi, D. (2019). *Monitoreando la inversión pública. El Impacto de MapaRegalías en Colombia*. BID.

Lewis-Faupel, S.; Neggers, Y.; Olken, B. A. y Pande, R. (2016). Can electronic procurement improve infrastructure provision? Evidence from public works in India and Indonesia. *American Economic Journal. Economic Policy,* 8(3), pp. 258-283.

Lizardo, R. (2018). *Gobierno electrónico y percepción sobre la corrupción. Un estudio comparativo sobre su relación en los países de Latinoamérica*. Universidad Complutense de Madrid.

Llinás, R. (2003). *El cerebro y el mito del yo*. Grupo Editorial Norma, Bogotá.

López Azumendi, S.; Facchina, M. y Zapata, E. (2021) Liderazgo público y participación privada y de ciudadanos: la transformación digital de la ciudad de Córdoba en Argentina. Policy Brief;24, Caracas: CAF. Recuperado de: **http://scioteca.caf.com/handle/123456789/1699**

Manual de Contrataciones Abiertas para el Estándar de Datos sobre Infraestructura — documentación de Open Contracting for Infrastructure Data Standards Toolkit - 0.9.3. (s. f.). Open-Contracting.Org. Recuperado de: **https://standard.open-contracting.org/infrastructure/latest/es/** (consulta realizada el 22 de octubre de 2021).

Makridakis, S. y Christodoulou, K. (2019). Blockchain: Current Challenges and Future Prospects/Applications. Future Internet. 11. 258. 10.3390/fi11120258.

Margetts, H. (2017). *In a digital society, governments should innovate with the best of them*. Foro Económico Mundial. **https://www.weforum.org/agenda/2017/02/digital-government-innovate-helen-margetts/**

Meeting new expectations. (27 de marzo de 2015). Deloitte.Com. **https://www2.deloitte.com/tr/en/pages/financial-services/articles/dcfs-know-your-customer.html**

Mendling, J.; Weber, I.; Aalst, W. V. D.; Brocke, J. V.; Cabanillas, C.; Daniel, F.; Debois, S.; Ciccio, C. D.; Dumas, M.; Dustdar, S.; Gal, A.; García-Bañuelos, L.; Governatori, G.; Hull, R.; Rosa, M. L.; Leopold, H.; Leymann, F.; Recker, J.; Reichert, M.; … Zhu, L. (2018). Blockchains for business process management – Challenges and opportunities. *ACM Transactions on Management Information Systems,* 9(1), pp. 1-16.

Miembros - Open Government Partnership. (1.º de marzo de 2019). Opengovpartnership.org. **https://www.opengovpartnership.org/es/our-members/**

MOE. (2018). Misión de Observación Electoral. *Democracias empeñadas. De financiadoras privadas a contratistas públicos.* Bogotá: Colombia. **https://www.moe.org.co/publicacion/democracias-empenadas/**

Moreno, A. y Teigland, R. (2018). *Blockchain, in The Rise and Development of FinTech 276* (Anonymous 1st).

Munidigital. (2021). Experiences. Munidigital.Tech. **https://en.munidigital.tech/case-studies**

Muralidharan, K.; Niehaus, P. y Sukhtankar, S. (2016). Building State Capacity: Evidence from Biometric Smartcards in India. *American Economic Review*, 106(10), pp. 2895-2929.

Muralidharan, K.; Niehaus, P. y Sukhtankar, S. (2020). Identity Verification Standards in Welfare Programs: Experimental Evidence from India. *NBER Working Paper, 26744.*

Muralidharan, K.; Niehaus, P.; Sukhtankar, S. y Weaver, J. (2021). Improving Last-Mile Service Delivery Using Phone-Based Monitoring. *American Economic Journal: Applied Economics*, 13(2), pp. 52-82.

Naciones Unidas. E-Gobierno Encuesta 2020. *Gobierno digital en la década de acción para el desarrollo sostenible.* (2020). Publicadministration.Un.Org; Departamento de Asuntos Económicos y Sociales de la ONU. **https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Spanish%20Edition).pdf**

Nakamoto, S. y bitcoin.org, W. (s. f.). *Bitcoin: A peer-to-peer electronic cash system*. Bitcoin.Org. Recuperado de: **https://bitcoin.org/bitcoin.pdf** (consulta realizada el 22 de octubre 2021).

Naudé, W. (2020). *Artificial intelligence versus COVID-19 in developing countries: Priorities and trade-offs.* UNU-WIDER.

Niforos, M.; Ramachandran, V. y Rehermann, T. (2017). *Block Chain: Opportunities for Private Enterprises in Emerging Market.* International Finance Corporation.

Nuffield Council on Bioethics. (2020). Beyond the exit strategy: ethical uses of data-driven *technology in the fight against COVID-19.* **https://www.nuffieldbioethics.org/publications/covid-19/webinar-beyond-the-exit-strategy-ethical-uses-of-data-driven-technology-in-the-fight-against-covid-19**

OCDE. (2003). *OECD E-Government Flagship Report "The E-Government Imperative"*. Public Management Committee.

OCDE. (2011). *The Role of Internet Intermediaries in Advancing Public Policy Objectives.*

OECD Publishing.

OCDE. (2016). Gobierno digital. En *Políticas de banda ancha para América Latina y el Caribe: Un manual para la economía digital.* OECD Publishing. https://doi.org/10.1787/9789264259027-15-es.

OCDE. (2017). SPECIAL FEATURE: Electronic services in tax administration. En *Revenue Statistics in Asian Countries 2017: Trends in Indonesia, Japan, Kazakhstan, Korea, Malaysia, the Philippines and Singapore.* OECD Publishing. **https://doi.org/10.1787/9789264278943-4-en**.

OCDE. (2019a). *Digital Government in Chile – Digital Identity.* OECD Digital Government Studies.

OCDE. (2019b). E-procurement to strengthen transparency and develop performance evaluation of public procurement in Kazakhstan. En *OECD Public Governance Reviews* (pp. 73-102). OCDE.

OCDE. (2019c). *Is there a role for blockchain in responsible supply chains?*

OCDE. (2019d). Aid by DAC members increases in 2019 with more aid to the poorest countries. https://www.oecd.org/dac/financing-sustainable-development/development-finance-data/ODA-2019-detailed-summary.pdf

OCDE. (2020). *Covid-19 en América Latina y el Caribe: Panorama de las respuestas de los gobiernos a la crisis.* OECD Publishing.

OCDE. (2021). *Guía de la OCDE sobre gobierno abierto para funcionarios públicos peruanos*

OCDE. https://www.oecd.org/gov/open-government/guia-de-la-ocde-sobre-gobierno-abierto-para-funcionarios-publicos-peruanos.htm

Olken, B. A. (2007). Monitoring corruption: Evidence from a field experiment in Indonesia. *The Journal of Political Economy*, 115(2), pp. 200-249.

Open contracting for infrastructure data standards toolkit — Open contracting for infrastructure data standards toolkit 0.9.3 documentation. (s. f.). Open-Contracting.Org. Recuperado de: https://standard.open-contracting.org/infrastructure/latest/en/ (consulta realizada el 22 de octubre de 2021).

OpenDataCharter. (2015). *Carta Internacional de Datos Abiertos*. https://opendatacharter.net/principles-es/

Ortega, D. (2019). 5 grandes preguntas sobre Big Data y Evaluación de Impacto. CAF. https:// www.caf.com/es/conocimiento/visiones/2019/03/5-grandes-preguntas-sobre-big-data-y-evaluacion-de-impacto/

Padilla, J. (2020). Blockchain y contratos inteligentes: aproximación a sus problemáticas y retos jurídicos. *Revista de Derecho Privado*, 39, pp. 175-201.

Paula, E. L.; Ladeira, M.; Carvalho, R. y Marzagao, T. (2017). "Deep Learning Anomaly Detection as Support Fraud Investigation in Brazilian Exports and Anti-Money Laundering," 15th IEEE International Conference on Machine Learning and Applications (ICMLA).

Peixoto, T. C.; Sifry, M. L.; Mellon, A. J. y Sjoberg, F. M. (s. f.). *Civic tech in the global south: Assessing technology for the public good*. World Bank Group. http://documents.worldbank.org/curated/en/717091503398213001/Civic-tech-in-the-global-south-assessing-technology-for-the-public-good

Peixoto, T. y Fox, J. (2016). *When Does ICT-Enabled Citizen Voice Lead to Government Responsiveness? WDR 2016 Background Paper*. Banco Mundial, Washington. https://openknowledge.worldbank.org/handle/10986/23650 License: CC BY 3.0 IGO

Peixoto, T. y Sifry, M. L. (2017). *Civic Tech in the Global South: Assessing Technology for the Public Good.* World Bank and Personal Democracy Press. https://openknowledge.worldbank.org/handle/10986/27947 License: CC BY 3.0 IGO

Persson, A.; Rothstein, B. y Teorell, J. (2013). Why Anticorruption Reforms Fail – Systemic Corruption as a Collective Action Problem. *Governance*, 26(3), pp. 449-471.

Pring, C. y Vrushi, J. (2019). *Barómetro Global de la corrupción en América Latina y el Caribe 2019 – Opiniones y experiencias de los ciudadanos en materia de corrupción* (Transparencia Internacional). https://transparenciacolombia.org.co/wp-content/uploads/gcb-lac-report-web.pdf

Puertas, A. M. y Teigland, R. (2018). Blockchain. En *The Rise and Development of FinTech* (pp. 276-308). Routledge.

Puthal, D.; Malik, N.; Mohanty, S. P.; Kougianos, E. y Das, G. (2018). Everything you wanted to know about the blockchain: Its promise, components, processes, and problems. I*EEE Consumer Electronics Magazine*, 7(4), pp. 6-14.

PwC. (2020). *Fighting fraud: A never-ending battle. PwC's Global Economic Crime and Fraud Survey*. **https://www.pwc.com/gx/en/forensics/gecs-2020/pdf/global-economic-crime-and-fraud-survey-2020.pdf**

Ramachandran, V. y Rehermann, T. (2017). *Can blockchain technology address DE-risking in emerging markets?* International Finance Corporation, Washington, DC.

RAMCC (2020). Paraná aplicará el software MuniArbol para registro y control del arbolado. Red Argentina de Municipios frente al Cambio Climático. Recuperado de: **https://ramcc.net/noticia.php?id=1075**

Raskin, M. (2017). The Law and Legality of Smart Contracts, *Georgetown Law Technology Review,* 2017, 1 Geo. L. Tech. Rev. Recuperado de: **https://georgetownlawtechreview.org/wp-content/uploads/2017/05/Raskin-1-GEO.-L.-TECH.-REV.-305-.pdf**

Right to Information. (2019). *Global Right to Information Rating Map*. Global Right to Information Rating. **https://www.rti-rating.org**

Rincón, E. (2020). *Derecho del comercio electrónico y de internet* (1.ª edición). Tirant lo Blanch. Rincón, E. (2021). *El desarrollo jurídico de Fintech. Las bases regulatorias de la Tecnología Financiera.* Tirant lo Blanch.

Ripani, L. y Roseth, B. (2021). ¿Qué significa el «futuro del trabajo» para los servidores públicos de América Latina y el Caribe? BID. **https://blogs.iadb.org/trabajo/es/futuro-del-trabajo-para-los-servidores-publicos/**

Romeu, J. y Rodríguez, J. (2013). *Publicidad y transparencia en la actividad contractual de las administraciones públicas.* **https://doi.org/0.13140/2.1.4309.2801**

Rosati, P. y Cuk, T. (2019). Blockchain Beyond Cryptocurrencies. In *Disrupting Finance* (pp. 149-170). Springer International Publishing.

Roseth, B.; Reyes, A. y Santiso, C. (2018). *Wait No More: Citizens, Red Tape and Digital Government*. Banco Interamericano de Desarrollo. **https://publications.iadb.org/en/wait-no-more-citizens-red-tape-and-digital-government-executive-summary**

Roseth, B.; Reyes, A. y Yee Amézaga, K. (2021). *Servicios públicos y gobierno digital durante la pandemia: perspectivas de los ciudadanos, los funcionarios y las instituciones públicas.* Banco Interamericano de Desarrollo. **http://dx.doi.org/10.18235/0003122**

Rossi, M.; Vásquez, A., y Cruz, J. (2020). *Divulgación de información y desempeño de la inversión pública: el caso de Costa Rica*. BID.

Rudin, C. (2012). Prediction: Machine Learning and Statistics. Spring. MIT OpenCourseWare, **https://ocw.mit.edu.** License: Creative Commons BY-NC-SA.

Ryvkin, D.; Serra, D. y Tremewan, J. (2017). I paid a bribe: An experiment on information sharing and extortionary corruption. *European Economic Review*, 94, pp. 1-22.

Santiso, C. (2020) El papel del Estado en la era digital post COVID-19. Recuperado de: **https://www.caf.com/es/conocimiento/visiones/2020/08/el-papel-del-estado-en-la-era-digital-post-covid19/**

Santiso, C. (27 de febrero de 2019). *Tecnología de integridad: tres formas en que los gobiernos pueden utilizar la tecnología para acabar con la corrupción.* apolitical. Recuperado de: **https://apolitical.co/solution-articles/es/tecnologia-de-integridad-interrumpir-la-corrupcion**

Santiso, C. (agosto de 2021). *La digitalización como estrategia anticorrupción.* Recuperado de: Santiso, C. y Ortiz de Artiñano, I. (2020). Govtech y el futuro gobierno. Caracas: CAF y PublicTechLab de IE University de España. Recuperado de: **http://scioteca.caf.com/ handle/123456789/1645**

Santiso, C. y Ortiz, I. (2020). Govtech y el futuro gobierno. Caracas: CAF y PublicTechLab de IE University de España. Recuperado de: **http://scioteca.caf.com/handle/123456789/1645**

Seco, A. (n. d.). *BLOCKCHAIN: Concepts and potential applications in the tax area (1/3)*. Ciat. Org. Recuperado de: **https://www.ciat.org/blockchain-concepts-and-potential-applications-in-the-tax-area-13/?lang=en** (consulta realizada el 22 de octubre de 2021).

Seco y Muñoz. (2018). Panorama del uso de las tecnologías y soluciones digitales innovadoras en la política y la gestión fiscal. Documento de trabajo, Washington, D.C.: IDB. Disponible en: **https://publications.iadb.org/publications/spanish/document/Panorama-del-uso-de-las-tecnolog%C3%ADas-y-soluciones-digitales-innovadoras-en-la-pol%C3%ADtica-y-la- gesti%C3%B3n-fiscal.pdf**

Shang, Q. y Price, A. (2019). A blockchain-based land titling project in the Republic of Georgia. Innovations: Technology, Governance, Globalization, MIT Press, vol. 12(3-4), pp. 72-78, Winter-Sp. **https://ideas.repec.org/a/tpr/inntgg/v12y2019i3-4p72-78.html**

Sheffer, A.; Pizzigatti, P y Soares, F. (2014). "Transparency Portals versus Open Government Data. An Assessment of Openness in Brazilian Municipalities," Proceedings of the 15th Annual International Conference on Digital Government Research.

Sheth, H. y Dattani, J. (2019). Overview of blockchain technology. *Asian Journal of Convergence in Technology*, 05(01), pp. 1-4.

Simon, C. y Blume, L. (1994) Mathematics for economists. W.W. Norton & Company Inc. New York.

Solon, L.; Rigitano, H.; Carvalho, R. y Souza, J. (2016). "Bayesian Networks on Income Tax Audit Selection. A Case Study of Brazilian Tax Administration. BMA@UAI, pp. 14-20.

Sooväli-Sepping, H. (Ed.). (2020). *Informe sobre desarrollo humano de Estonia 2019/2020.* **https://inimareng.ee/en/info.html**

Strusani, D. y Houngbonon, G. V. (2019). The Role of Artificial Intelligence in Supporting Development in Emerging Markets. EMCompass,no. 69;. International Finance Corporation, Washington, DC. **https://openknowledge.worldbank.org/handle/10986/32365**

Superintendencia Financiera de Colombia, Circular Externa 027 de 2020.

Szabo, N. (1996) Smart Contracts: Building Blocks for Digital Markets **https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html**

Thackeray, J. (2019). *What are the Inherent Risks Associated with Cryptocurrency?* **https://support.niftys.com/hc/en-us/articles/4405752761115-What-are-the-risks-with-buying-selling-NFTs-**

The World Wide Web Foundation. (2018). *Open Data Barometer.* Leaders Edition. From Promises to Progress. Washington DC: World Wide Web Foundation. Recuperado de: **https://opendatabarometer.org/doc/leadersEdition/ODB-leadersEdition-Report.pdf**

Tiatasin, K. "IT Risk Management for E-Government Implementation Success" N.A. **http://www.jba.tbs.tu.ac.th/files/Jba135/Article/JBA135KrongSiri.pdf**

Transparencia Internacional. (2017). *Las personas y la corrupción. América Latina y el Caribe. Barómetro Global de la Corrupción.* Coralie Pring, editora. Berlín, Alemania. Recuperado de: **https://www.transparency.org/en/publications/global-corruption-barometer-people-and-corruption-latin-america-and-the-car**

Transparencia Internacional. (2019). *Barómetro Global de la Corrupción en América Latina y el Caribe 2019. Opiniones y experiencia de los ciudadanos en materia de corrupción*. Coralie Pring, Jon Vrushi, editores. Recuperado de: **https://images.transparencycdn.org/images/2019_GCB_LAC_Report_EN1.pdf**

Transparencia Internacional. (2021). CPI 2021 for the Americas: A Region In Crisis. **https://www.transparency.org/en/news/cpi-2021-americas-a-region-in-crisis**

Transparencia por Colombia y Monitor Ciudadano de la Corrupción. (2019). *Así se mueve la corrupción: Radiografía de los hechos de corrupción en Colombia 2016-2020.* Bogotá D.C., Colombia. Recuperado de: **https://www.monitorciudadano.co/documentos/hc-informes/2021/Radiografia-2016-2021.pdf**

Treshock, M. (2020). How the FDA is piloting blockchain for the pharmaceutical supply chain. **https://www.ibm.com/blogs/blockchain/2020/05/how-the-fda-is-piloting-blockchain-for-the-pharmaceutical-supply-chain/**

U.S. v. Sheirer, United States Court of Appeals, Tenth Circuit, 13 de julio de 1990. **https://www.casemine.com/judgement/us/5914898badd7b0493450420c#**

U.S. America, Plaintiff, v. Robert J. Riggs, also known as Robert Johnson, also known as Prophet, and Craig Neidorf, also known as Knight Lightning, Defendants. N.º 90 CR 0070. United States District Court, N.D. Illinois, E.D. 5 de junio de 1990. **https://law.justia.com/cases/federal/district-courts/FSupp/739/414/1610447/**

Valle-Cruz, D.; Sandoval, R. y Gil-García, J. R. (2016). "Citizens' perceptions of the impact of information technology use on transparency, efficiency and corruption in local governments," Information Polity, 21(3), pp. 321-334.

Van Eeten, M. (2017). "Patching security governance: An empirical view of emergent governance mechanisms for cybersecurity", Digital Policy, Regulation and Governance, Vol. 19, n.º 6, pp. 429-448. **https://doi.org/10.1108/DPRG-05-2017-0029**

Van Niekerk, M. (2021). How blockchain can help dismantle corruption in government services. Foro Económico Mundial. **https://www.weforum.org/agenda/2021/07/blockchain-for-government-systems-anti-corruption/**

Varian, H. (1992). Microeconomic Analysis. New York: Norton.

Volosin, N. (2015). *Open data, corruption and public procurement.* Montevideo: Iniciativa Latinoamericana por los Datos Abiertos (ILDA). Recuperado de: **https://zenodo.org/record/4562395#.YLd4ay0RppS**

Wachter, S. y Mittelstadt, B. (2018). *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*. Columbia Business Law Review. **https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829**

Waller, M.A. y Fawcett, S.E. (2013). Data Science, Predictive Analytics, and Big Data: A Revolution That Will Transform Supply Chain Design and Management. J Bus Logist, 34: pp. 77-84. **doi:10.1111/ jbl.12010**

Wilms, G. European University Institute, "Good data protection practice in research". (Abril de 2019). **https://www.eui.eu/documents/servicesadmin/deanofstudies/researchethics/guide-data-protection-research.pdf**

Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. World Bank. (2017). Registering Property: Using information to curb corruption. En *Doing Business* (pp. 51-55). Banco Mundial.

Zamboni, Y. y Litschig, S. (2018). "Audit risk and rent extraction: Evidence from a randomized evaluation in Brazil". *Journal of Development Economics*, 134, pp. 133-149.

Zapata, E.; Scrollini, F. y Fumega, S. (2020). ¿Cuán abiertos están los datos públicos? *El Barómetro de Datos Abiertos para América Latina y el Caribe 2020*. Recuperado de: **https://scioteca.caf.com/handle/123456789/1710**

Zuboff, S. (2019). The age of surveillance capitalism: the fight for a human future at the new frontier of power. New York: Public Affairs.

Zuleta, M. (2019). *Hacia una política de datos abiertos del Sistema de Compra Pública para los países miembros de la RICG.* Montevideo: Iniciativa Latinoamericana por los Datos Abiertos (ILDA). **http://doi.org/10.5281/zenodo.4318938**

CAF BANCO DE DESARROLLO
DE AMÉRICA LATINA