July, 2020

Good ID in Latin America

Strengthening appropriate uses of Digital Identity in the region

Authors
Alexandre Barbosa
Celina Carvalho
Cláudio Machado
Janaina Costa

Table of contents

Acknowledgments

We would like to thank Omidyar Network for supporting this research project, not only financially, but also networking with colleagues from the Global South working on digital identity. We are also grateful to our peers at the Center for Internet and Society (CIS), in India, and at the Center for Intellectual Property and Information Technology Law (CIPIT) for thoughtful discussions and cooperation. We are moving toward strengthening the Good ID movement.

Expert contributors

This report draws on the expertise and inputs of the following expert contributors:

Fabro Steibel • Executive Director, ITS Rio
Alejandro Barros • International Consultant on Digital Development Public Policy
Edgar Vásquez Cruz • IT solutions provider
Evelyn Téllez Carvajal • Researcher, INFOTEC Mexico
Fernanda da Escóssia • Journalist and university professor, IBMEC Rio
José Villalba • CEO, Electronic-ID
Juan Carlos Lara • Director of Research and Public Policy, Derechos Digitales
Miguel Arce • Commercial Manager, Pagos Digitales Peruanos
Miguel Morachimo • Executive Director, Hiperderecho
Raquel Chrispino • Judge of law, Court of Justice of the State of Rio de Janeiro
Ricardo Saavedra • Digital Registration and Certification Manager, RENIEC

Editing

Celina Bottino • Project Director, ITS Rio
Clara Langevin • Graduate Consultant, Columbia University

Design project

Ana Luisa Figueiredo • ITS Rio

Photos

Tales Duarte • ITS Rio
Agência Brasil

Funded by
OMIDYAR NETWORK

ITS
Instituto
de Tecnologia
& Sociedade
do Rio

Abbreviations and acronyms

AFIS	Automated Fingerprint Identification System
CadÚnico	Unified Registry for Social Programs
CEDN	Coordination of the National Digital Strategy
CEN	Electronic Birth Certificate
CEV	Electronic Vaccination Card
CR	Civil Registration
CRVS	Civil Registration and Vital Statistic
CURP	Unique Population Registry Code
CDD	Customer Due Diligence
DNI	National Identity Document
ID4D	Identification for Development
ICT	Information and Communication Technologies
INFOTEC ICT	Research and Innovation Center of Mexico
KYC	Know-Your-Customer
MIS	Management Information System
NHDID	National Health Digital Identifier
OEA	Organization of American States
OECD	Organization for Economic Cooperation and Development
PAHO	Pan American Health Organization
PBF	Bolsa Família
RENIEC	National Registry of Identification and Civil Status
SDG	Sustainable Development Goals
SID	Sistema de Identidad Digital
SPP	Social Protection Programs
UN	United Nations
UNAIDS	Joint United Nations Programme on HIV/AIDS
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNSD	United Nations Statistics Division
UDHR	Universal Declaration of Human Rights
WHO	World Health Organization

Executive Summary

Photo: Agência Brasil

Executive summary

The digital transformation of the economy and society is a reality. Thus, digital identity is under the limelight as an essential element of the future. Under the same analogical logic, one must easily be able to digitally prove (or demonstrate) who they are, or risk being excluded from the future.

Although digital transformation does carry many opportunities, it is not the panacea for Latin American problems. Disruptive technologies, innovative approaches, and, above all, new user expectations enter the arena in which old issues remain. Regarding identification, the needy and vulnerable population continues facing barriers to have access to basic personal documentation, weak privacy and data protection practices, a highly centralized identification system architecture, and low utilization of identification to improve the delivery of services.

Concomitantly, the challenge of how to identify individuals while assuring their rights, duties, and control over data increases in tandem. Moreover, identification can vary considerably in its conceptualization, legal and organizational arrangements, and operational and technological infrastructure. It is becoming a buzzword, used differently in accordance with political agendas.

In addition, key issues such as exclusion, discrimination, and surveillance cannot be overlooked. These were used as a base for this report, adapted to a Latin American perspective. The guiding principle of this study is inclusion, and this will be used as a lens to our analysis.

With the rise in the adoption and promotion of national digital identity systems worldwide, concerns arise on how to ensure their appropriate use. Both sectoral and regional approaches are needed to truly address the traditional and emerging challenges of inclusion and privacy. In partnership with Omidyar Network, the ITS Innovation team, through a yearlong research project, designed an analysis to identify regional Good ID frameworks and strategically foster appropriate practices in sectoral uses of digital ID. To do so, this research project has three main objectives:

- To investigate the appropriate uses of digital identity in specific sectors, such as current identification practices and the circumstances where digital identification can be risky to individual rights.
- To map principles and determine guidelines for the conception,

adjustment, and implementation of digital identification for sustainable development in Latin America, hence, by placing inclusion, safe systems, and good governance at the core of the agenda.

- To support policymakers and practitioners in Latin America to implement the principles of a good, hence inclusive, identification system and, thus, to strengthen and consolidate the Good ID movement on the continent.

To substantiate our objectives, we conducted a vast review of the literature to understand digital ID as a phenomenon and the stakeholders involved. We then assessed the different impacts and relations of digital identification in specific sectoral use cases. Finally, we interviewed a sample of stakeholders from Mexico, Chile, Peru, and Brazil to back up those specific case studies.

Our results are structured upon use cases to understand how an identification system should work in these specific contexts and interrelate with the impacts of digital ID. The sectors selected were digital **government services**, **financial inclusion, healthcare**, and **social protection**. This approach was necessary due to the complexity of the issue, and establishing a single answer for all sectoral use cases would be a frivolous approach. As key takeaways for the appropriate uses in the sectors we highlighted the following:

Digital Government Services

Several countries worldwide are developing and implementing national and regional digital government agendas. The way people will “log into” these platforms and the full value of participatory mechanisms is determined by a digital identification. Thus, digital ID may decrease or increase the distance between state and society and enhance or diminish trust in the public sector. Key takeaways:

1. **Digital Government Services should encompass, as their very first step, a widely accessible identification system that adds value to the user by simplifying procedures, reducing direct and indirect costs, and enabling transaction services.**
2. **Integrated or federated authentication structures that use shared data from different systems should follow and incorporate robust transparency practices and inform the users about the treatment of their personal data, pursuant to the national data protection law or, in the absence of such law, by following international best practices.**
3. **Digital Government Services should reach the most vulnerable groups, so there should be a costless digital identification option**

for those users. Regardless of the required level of assurance of a given digital government service, digital credentials should be same and inclusive to users, ideally by means of costless digital credentials.

Financial Inclusion

Identification is key for determining customer reliability and reducing fraud. Digital ID can be an enabler of efficient and simpler Know Your Customer (KYC) procedures, hence enabling financial inclusion. It may also support anti-money laundering and counter-terrorism policies and systems. It has gained more attention with the rise of open banking (i.e. financial and personal data sharing among financial institutions) worldwide. Key takeaways:

1. **Basic KYC requirements must ideally be costless for the target population's financial inclusion and be easy to perform. It is important to clearly separate the basic data used to identify someone based on the complementary information required for access to specific services and customer due diligence.**
2. **As the leading sector in identification from a technological perspective, financial technology companies and large banks should support and be key drivers of privacy-enhancing technologies. In addition, the inexistence of redress and grievance mechanisms to access the history of one's data is an important indicator of bad practice, given the sector's technological maturity.**
3. **Financial regulators should work closely with identification and data protection authorities ensuring interoperability with the national identification system.**

Healthcare

Identification involves several important issues, from the universal right to healthcare to patient safety and efficiency in the delivery of public services. Correct identification helps to prevent a patient from receiving inappropriate treatment, such as administering a drug the patient is allergic to, for example. Digital ID may also facilitate the issuance of aggregated electronic records and generate data to support evidence-based health policies. Key takeaways:

1. **If a unique national identification for health services is established, it may be linked to a foundational ID. This link, however, should not allow access to sensitive medical data by third parties. When required to meet public health information needs, data should be anonymized, preventing the patient from being reidentified.**

2. **Access to urgent medical services, not only emergencies, should never be conditioned to identification. Hence, that is the case for Digital ID.**
3. **Alternative identification methods may need to be developed to ensure the integrity of the application process for national schemes that require identification (such as vaccination programs). Digital ID could support that.**

Social Protection

Identification is often required to prove eligibility for programs such as cash transfers, pensions, ration cards, social security, and other programs. This is a problem since those most in need of such assistance are also those least likely to have an identity document, including needy, rural, and marginalized people. Hence, digital ID is seen as a solution for weak identification systems as a way of overcoming the problem, also by facilitating beneficiaries' enrollment and government-to-people transactions. However, especially in developing countries, this can be problematic (i.e. neglection of the fundamental role played by basic documentation).

1. **Governments should create a single registry for social protection, adopting an inclusive perspective to improve their capacity to reach the vulnerable population. It is crucial to simplify and to make identification services more accessible to the undocumented population by balancing requirements and the beneficiaries' conditions.**
2. **The integration of Management Information Systems and digital identification schemes must take into consideration the risk of excluding the most vulnerable population, while yet targeting policy effectiveness.**
3. **The adoption of biometric technology in social protection needs to be preceded by a holistic assessment of the national identification system, in which institutional and legal frameworks should be evaluated through the lenses of promoting inclusion and rights, ensuring that the needy and most vulnerable are not excluded.**

Section 1

Latin America and Identification in the Digital Age

Photo: Agência Brasil

1. Latin America and Identification in the Digital Age

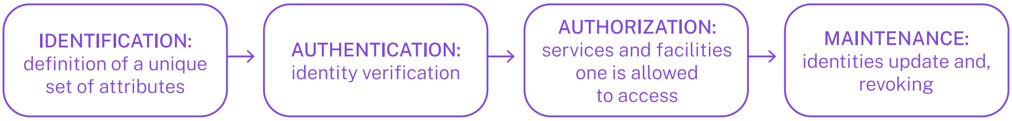
1.1. Digital Identity at a glance

In the past few decades, two perspectives on identifying individuals in the digital age have stood out in the literature on Digital ID. One perceives digital identities, combined with emerging technologies, as a tool for mass surveillance, thus, they are seen with distrust. The other views the digitalization of identity systems as a means to strengthen rights and improve access to services.

The point is that Digital ID can mean different things: It can be defined as a set of electronically captured and stored attributes (e.g.: name, gender, date of birth, and biometric data, such as an iris scan, fingerprints, and facial, among others) and/or credentials (e.g.: PINs, ID cards, mobile applications) that uniquely identify a person. Nevertheless, we support a more systemic view of digital ID, one that goes beyond digital authentication, or a website log in, a mobile-based legal identity, digital certificates, or electronic birth records in isolation.

To us, Digital ID is a technical mechanism for the digital and secure identification of individuals in which there is no face-to-face contact. In a foundational identity system (World Bank, 2018d)[1], digital identity must be based on a responsible institution, consistent legislation, and on technical means that allow for interoperability with different information systems. In other words, it is assumed that digital identity inherits the same desirable characteristics as civil identification, i.e., it is inclusive, accessible, portable, and persistent.

Figure 1: dentity Management Lifecycle


IDENTIFICATION:
definition of a unique set of attributes
AUTHENTICATION:
identity verification
AUTHORIZATION:
services and facilities one is allowed to access
MAINTENANCE:
identities update and, revoking

Source: Own elaboration

Traditional identity management is usually divided into four steps: (i) registration or identification, (ii) authentication, (iii) authorization, and (iv) maintenance. Each has specific stages, for example, the former encompasses the issuance, use and management of personal identities (including identity data collection, validation through the proof and deduplication of identity and the issuing of credentials). Identification is related to the process of one stating or asserting who they claim to be. Insofar as authentication and authorization are concerned, it is worth highlighting the distinctions there are between the two. Authentication is the validation of identity. It should ensure a person is real (human) and singular (unique); however, while identification can be public information, authentication must be private. The latter is usually associated with something you have (e.g.: a physical token), something you know (e.g.: a password), and something you are (e.g.: fingerprints). 'Something you are' is becoming increasingly relevant with the maturity of biometric technology, such as facial identification.

When a person is verified and authenticated in a transaction, it is important to determine which specific services or facilities he or she can have access to. The process of determining this eligibility is called authorization. It can be argued that each of these stages becomes more challenging in fully digital, or even hybrid, systems. Finally, there is the maintenance step, which is associated with the possibility to update or revoke identities and credentials.

Risks and Balance

Digital identity schemes are prone to risks of adverse consequences and mission creep (Bhadra, 2019). Firstly, the scheme itself can be distorted and exclude part of the population, and it may violate fundamental rights, such as access to basic services and privacy. So, there are risks of legal, cultural, economic, and technological exclusion (World Bank, 2019b).

In addition, the digital gap remains a barrier to many people in developing nations, and digital literacy engenders even greater risks of exclusion of needy and vulnerable populations. Many digital identity projects rely on mobile applications and, therefore, require significant levels of connectivity and access to technological devices. In this regard, if not carefully implemented and disseminated, those programs tend to increase the digital and social divide (Ratcliffe, 2019).

Finally, identity data sensitivity is worthy of note, and this may be deepened when it comes to sectoral uses, such as for healthcare. The risk of information misuse increases with digitization. Unauthorized access to or misuse of personal information can reduce trust, undermine privacy rights, promote discrimination, and, in some cases, put vulnerable groups at a serious risk of harm (World Bank, 2019b). Regardless of a consensus on the subject, it is necessary to pursue a balanced approach, one in which the risks arising from adopting digital identity systems are mitigated.

Principles

UN SDG 16.9 states that everyone is entitled to legal identity, but there is no fit for all identification scheme. It is impractical to advocate for a unique digital identity system model, but it is crucial to inform stakeholders about certain guiding principles, technical options, and good practices, so that the system can be best adapted to the needs, objectives, and context.[2]

Governments, international multilateral bodies, the private sector, and civil society organizations have been addressing the digital identification schemes and their potential risks and opportunities. As a result, some principles have been set to mitigate the aforementioned risks and enhance benefits and opportunities when implementing a digital identification system.

In this sense, we highlight the work done by a group of international organizations facilitated by the World Bank and the Center for Global Development, which contributed to the debate with the Principles on Identification for Sustainable Development (World Bank, 2016). To serve higher-level outcomes, they assembled guiding principles into three pillars: i) fostering inclusion, through universal identity coverage and accessibility; ii) establishing an accurate, secure, responsive, and sustainable design, and iii) ensuring good governance and building trust by protecting privacy and user rights.

In addition, the Good ID movement, a multi-sector coalition, is also helping to inform policy, technology design, and practice on the subject in all regions[3], advocating for systems that guarantee privacy, inclusion, user value, user control, and security.

This work aims to contribute to the promotion and understanding of the application of these principles within the sectoral uses of digital identity analyzed in the Latin American context.

Sectoral Uses of Digital Identity

There is a distinction between “functional” and “foundational” DID systems. Functional systems generate identities to serve a specific function in a given sector. These systems support the delivery or authorization of a specific service and may or not be linked to ID systems that support other functions. Any given person may have a variety of functional IDs (e.g., driver’s license, health insurance card, voter registration card). Foundational systems, in contrast, are intended primarily to provide identity as a public good, not to supply a specific service.[4]

Digital ID schemes have different characteristics, functionalities, and risks according to their use. In this paper, we will present a few examples, addressing their uses with regard to digital government, financial services, healthcare, and social protection.

There are several other sectoral use cases for digital identification that will not be addressed herein. For instance, many countries have their civil identification associated with their electoral agenda. A recurrently mentioned and consolidated case is Estonia's electronic voting system. Regarding fiscal systems, digital ID has a strong potential for facilitating tax payment and collection through People-to-Government (P2G) transactions and for preventing tax evasion. Therefore, it can propel state capacity (Gelb, A. *et. al.*, 2020). These are just a few of the many industry uses for digital identities.

1.2. Inclusion at the Core

> Identity is a right, and it should be extended to everyone. Nevertheless, this does not mean that identification should be mandatory; however, anyone who desires to be identified by the system, should be able to.

The right to identity is not only a "passport" to other rights, rather a right *per se*. Personal identity is intrinsically linked to the rights to a nationality and to the right to recognition everywhere as a person before the law. These are recognized as a human right by the international community (Universal Declaration of Human Rights, 1948) and must be protected by robust institutional and legal frameworks.

Civil Registration and Vital Statistics

According to the United Nations Statistics Division (UNSD), Civil Registration and Vital Statistics (CRVS) is the continuous, permanent, compulsory, and universal registration of the occurrence and characteristics of vital events of the population in accordance with the law.

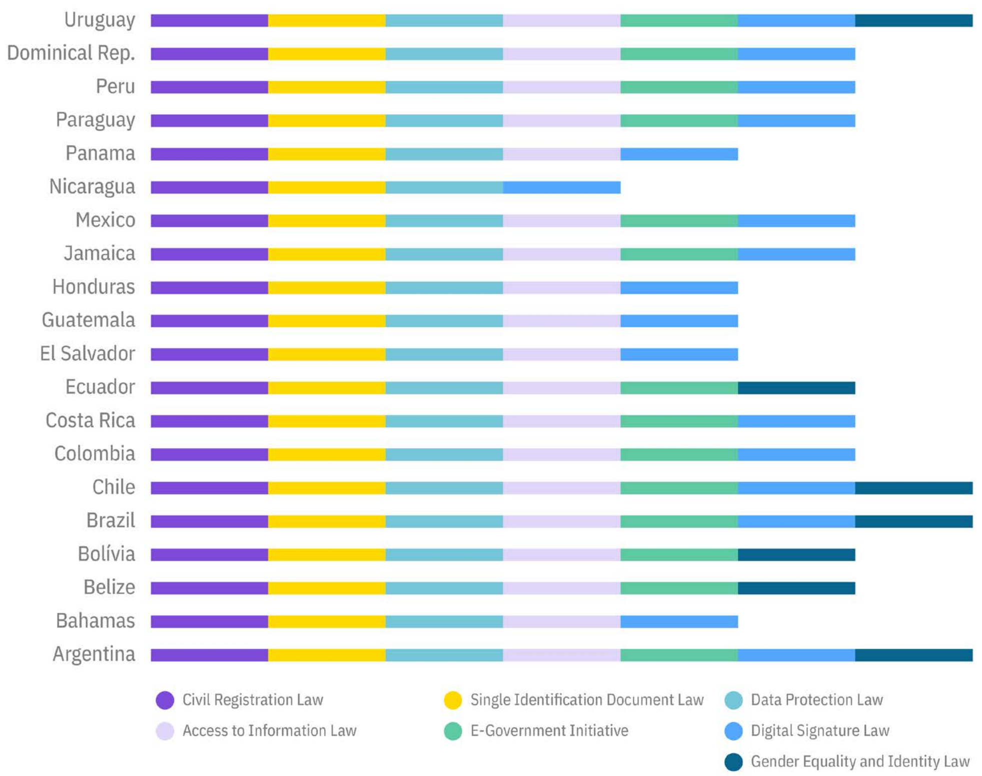
The UN Legal Identity Expert Group recommends linking CRVS and ID because the CRVS system plays a crucial role in a legal framework as the official means to prove the biographic information needed to certify many human rights, such as the right to a name and parentage. Additionally, by integrating CR and ID, there may be a holistic view (cradle-to-grave) of individuals showing how an organic link between the systems could improve identity management services and push service delivery to citizens.

However, in some contexts it may be difficult to integrate CRVS and ID.

Latin American countries have very advanced and comprehensive legislations regarding identification and data protection. To provide an overview of the legislative framework, the following chart shows which countries regulate i) civil registration; ii) the issuing of a single identification document; iii) the protection of personal data; iv) access to information; v) electronic government; vi) digital signature, and vii) gender equality and identity. Digital identification schemes create new possibilities and risks for individuals.

Although institutional recognition of identity as a right and data protection legislation are essential, complementary safeguards may be necessary to ensure compliance and an inclusive digital identification system. For instance, a user-centric approach, placing individuals at the heart of digital identity and in control of when, how, and if they wish to assert their identities

Figure 2: Legal frameworks by country



Source: Adapted from Civil Registries and Identification Offices: Analysis and Country Records, Inter American Development Bank (IADB), Estefania Calderón, 2019, <*Registros civiles y oficinas de identificación: análisis y fichas de país*>

online, is paramount (GSMA, 2016). These safeguards should be understood as rooted in an institutional and legal framework broader than autonomous technological solutions, from the protection of rights and socioeconomic inclusion perspective.

Additionally, it is worth noting that in some contexts and in many historical examples, identification could put an individual in danger of violence or exclusion. Intentionally or not, identification schemes can facilitate the persecution of groups belonging to a given religion, ethnicity, gender or political ideology and contribute to the stigmatization of individuals (e.g. exposure of a disease status or a situation of economic vulnerability to prove eligibility for a social benefit).

Digitization does not eliminate the aforementioned risks and might add others. Digital identification schemes can add noticeable risks of exclusion to poor and vulnerable populations. Digital access and literacy are key. Nevertheless, the digital gap remains a challenge worldwide, especially in developing nations. That is why it is paramount to have a clear digital identification design to promote inclusion in all its dimensions and strengthen safeguards for everyone. A system cannot be classified as Good ID without this.

Universal coverage

The United Nations Global Goals for Sustainable Development call for all individuals to have official proof of their identity by 2030 (Target 16.9). By establishing this target, the United Nations did not make identity schemes mandatory for all, but recognized everyone has the right to identity. The difference between universal coverage and mandatory identity is not a word game. A Good ID implementation means a digital identity scheme that enables the inclusion of all individuals to fully participate in the society and economy they live in. However, it is notorious that the process faces many key challenges to be inclusive rather than exclusive.

Furthermore, the country's Information and Communication Technology (ICT) and data infrastructures are critical elements. A minimal level of ICT infrastructure for providing digital identity should be considered in such a manner as to make it possible to include all residents of a country. The policy should also consider remote populations that have low infrastructure access rates and suffer with the digital divide.

Multichannel and priorities

Digital identities and traditional identification mechanisms can coexist. It may not be possible to fully replace physical personal documents by a digital scheme in many countries. At the same time, individuals should also have access to alternative means of identification and choices in how they identify themselves. Therefore, a multichannel approach should be considered in countries where there is no guarantee of a minimum level of ICT infrastructure nationwide.

A point of attention for this hybrid system is that it may start a process of differentiation between those who have access to Digital ID-enabled services and those who are kept in the physical system. For instance, if digital services were more efficient than face-to-face services, that would increase the inequality engendered by the digital gap.

Gender balance

Proof of age and identity can be crucial to ensure women's independence and financial inclusion, as well as being a tool to protect girls from child marriage[5] and trafficking. However, gender inequality is very present in the inclusion, civil registration, and vital record statistics. According to the Center of Excellence for CRVS Systems, women are more negatively affected by death records and subject to greater difficulties in registering their children than men (Centre of Excellence for CRVS Systems, 2020).

This means they face greater barriers and are underrepresented in vital statistics, such as those used in public policies to reduce female mortality, for example. In addition, marriage, divorce, and death records are needed for women to secure pension benefits and claim inheritance rights. The digitization of identity must address these concerns.

Accessibility

A good identification system is designed for its context and ensures proper access for users and the decent functioning of the system. When these aspects fail, a large portion of society may be excluded from accessing vital services. Therefore, it is important to consider what the minimum standard for infrastructure should be and how the system will address, in particular, minorities and vulnerable individuals. That is, it should not exclude, by default, people who have a lower level of digital literacy[6] or those with socioeconomic difficulties in accessing digital media, such as rural, riverine, indigenous, and maroon communities.

1.3. Digital ID in Latin America

Latin America has played an important role in the development of modern identification technologies, especially in the improvement of Dactyloscopy (fingerprint) technology (Ferrari, 2015). Juan Vucetich and his collaborators in La Plata, Argentina, improved the method and designed a new perspective on the use of fingerprints in a non-criminal context.[7] Dactyloscopy was simpler to use and more effective than the Bertillonage system, created by Alphonse Bertillon, in France, and adopted, in the 20th century, as the official method for criminal and civil identification in almost all Latin American countries. The Vucetich approach was the hegemonic benchmark before identification started to be automated using the Automated Fingerprint Identification System (AFIS) during the 1970s. This goes to show that Latin America has always been open to innovations in identification technology, so, logically, players in the region are currently looking to digital IDs for application in many sectors.

That said, the success of any national program, digital or not, depends more on the process and context rather than on the technology. The country's political situation and the government's capacity to implement a given system cannot be overlooked. In addition, other factors to be considered are also the environment, culture, history of conflict, and poverty levels. Thus, in this section we provide an overview of the interrelation between these factors and identity in the region.

Regional and Cultural Aspects of Identification

A person's identification can be perceived as a right *per se* or, conversely, as an underpinning of the right to privacy. Latin American countries, in their own historical context, also crossed this dichotomy in the development of their identification systems. Unlike other countries in the Global South, Latin America has a remarkably similar cultural, religious, and colonial heritage. This common ground is reflected in how identification is perceived in the region.

Forty years before the United Nations Universal Declaration of Human Rights, Vucetich (1916) mentions "the right to a name". Be it a historical anachronism or not, and regardless of a precise definition of a "right to identity", it is undeniable that Vucetich argumentation was very innovative in comparison to others identifications pioneers. He argued during the drafting of the Law of People's Identity Registry, in Argentina, that the the identification of all inhabitants, without any distinction, would be an important step to guarantee the fulfillment of the right to name and to ensure the proper functioning of State institutions and, consequently, for the good of society. This may be perceived as the benchmark recognition of the right to identity in the region.[8]

Additionally, the anthropologist Mariza Peirano inquired about the social and cultural meanings of personal documents in Brazil (Peirano, 2009). Her research adopted an innovative approach and highlighted that the documents were not limited to their formal and bureaucratic use, but have great symbolic meaning to people. The Employment and Social Security Record Card is much more than an employment record book, it splits the population into honest people and *"vagabundos"* (vagrants). She concludes that 'documents create the citizen,' in people's subjective perception.

In this sense, the work of Fernanda da Escóssia is very relevant for the topic in Latin America (Escóssia, 2019a). Her doctoral thesis was about the lives of unregistered people in the city of Rio de Janeiro. She investigates an individual's perception when they lack legal proof of identity, demonstrating that they do not see themselves as human beings.

"(...) I discovered that those people felt very deprived of the notion of 'I am a person,' 'I have rights.' Many of them used to tell me they felt like a dog...' 'I am nobody." She emphasized that civil registration is a precondition for a "sense of better existence" (Escóssia, 2019b).

Proof of identity, in this regard, is not only about owning a piece of paper, or a mobile application. It is the actual possibility of having your existence officially recognized by the state. As her research demonstrates, for many of those who lack civil registration, securing it is a step in the path toward dignity.

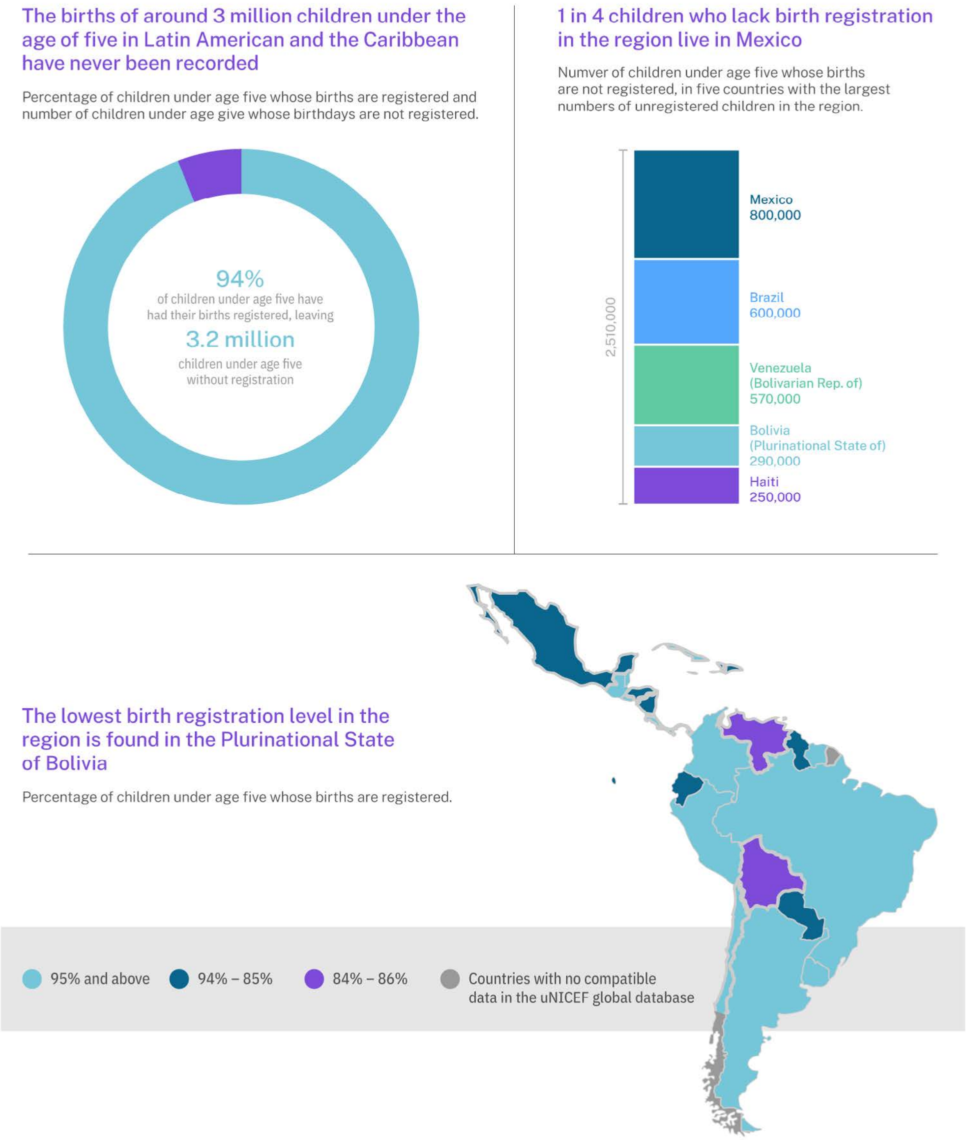
Nevertheless, it is important to highlight that identity management in the region is usually carried out by a central identification authority for enrollment and the issuance of credentials. Unfortunately, as most Latin American countries were governed by dictatorships in the second half of the last century, ID systems were often appropriated for surveillance and persecution (e.g. biometric identification facilitated the persecution of opponents of the regime). Thus, the paradoxical history of identification in Latin American countries shows how identification can be used for good and bad purposes.

Identification Going Digital in the Region

As previously indicated, the first step of an identity system is the individual's civil registration for issuing legal identity. In this sense, UNICEF data show that Latin America still faces a great challenge to reach universal birth registration (UNICEF, 2016).(fig.3)

In Latin America, there is a significant number of ethnic minority groups. One study carried out by the Organization of American States (OAS) concluded that the one key factor that affected under-registration was the existence of legal barriers for registration using ethnic names (OEA, 2008). Likewise, a UNICEF report also highlights how certain groups may face additional barriers to be included in the civil registry (UNICEF, 2016). It is worth noting that rural children from the Amazon region accounted for approximately 10

Figure 3 : Birth registration statistics in Latin America



The births of around 3 million children under the age of five in Latin American and the Caribbean have never been recorded

Percentage of children under age five whose births are registered and number of children under age give whose birthdays are not registered.

1 in 4 children who lack birth registration in the region live in Mexico

Numver of children under age five whose births are not registered, in five countries with the largest numbers of unregistered children in the region.

2,510,000
Mexico 800,000
Brazil 600,000
Venezuela (Bolivarian Rep. of) 570,000
Bolivia (Plurinational State of) 290,000
Haiti 250,000

The lowest birth registration level in the region is found in the Plurinational State of Bolivia

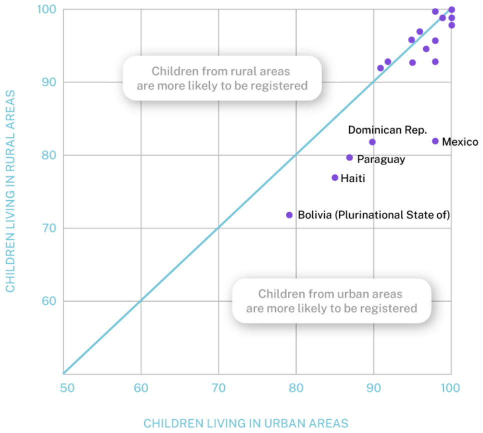
Percentage of children under age five whose births are registered.

● 95% and above
● 94% – 85%
● 84% – 86%
● Countries with no compatible data in the uNICEF global database

Source: Reprinted from Birth Registration in Latin America and the Caribbean: Closing The Gaps, UNICEF, 2016, <*Birth Registration in Latin America and the Caribbean: Closing The Gaps*>

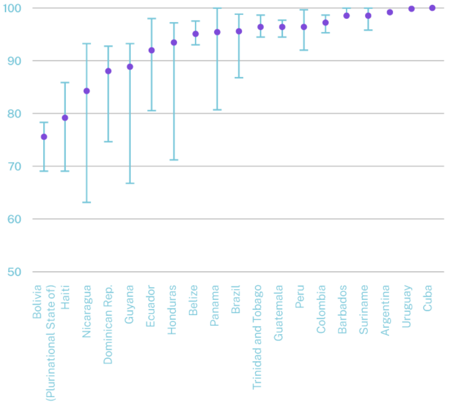
percent of those without identification in 2015 (Center for Global Development, 2017b). This shows how the registration process itself often lacks sensitivity to provide for the inclusion of indigenous and riverine populations. Urban-rural differences also mask deeper underlying disparities, mainly related to poverty. In addition, excluded populations, such as undocumented migrants, are often unaware of their rights regarding birth registration or may be reluctant to register their children for fear of deportation to their country

Figure 4 : In countries with lower overall levels, birth registration is more common in urban than rural areas; where levels are higher, disparities due to place of residence diminish



Source: Reprinted from Birth Registration in Latin America and the Caribbean: Closing The Gaps, UNICEF, 2016, <*Birth Registration in Latin America and the Caribbean: Closing The Gaps*>

Figure 5 : National birth registration prevalence may hide important geographic disparities



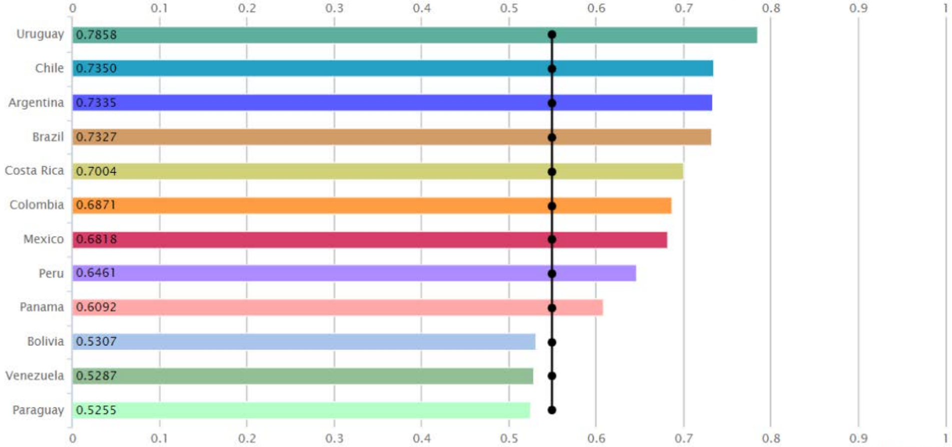
Source: Reprinted from Birth Registration in Latin America and the Caribbean: Closing The Gaps, UNICEF, 2016, <*Birth Registration in Latin America and the Caribbean: Closing The Gaps*>

of origin (UNICEF, 2016). These access barriers often remain or increase with digital identification, which has gained importance as a key to gain access to rights and services in the digital world.

Moreover, the need to improve public management and respond to citizens' needs is also driving the promotion of digital identity as an essential tool for the inclusion and reduction of transaction costs in the entire economy, thus contributing to improving the quality of services, both in the public and private sector (IADB, 2019; IADB, 2017).

That said, digital transformation is taking place everywhere, including in Latin American countries. Despite the regional similarities, the pace of digitization and the impact on society and on the public sector is proportional to their Human Development Indexes. For instance, the Electronic Government Development Index developed by the United Nations[9] demonstrates that countries like Uruguay (which has a very high index), Chile, Argentina, Brazil, and Costa Rica score over 0.7 out of 1, others rate really low, such as Haiti (0.34) and Nicaragua (0.42).[10]

Figure 6 : UN Electronic Government Development Index

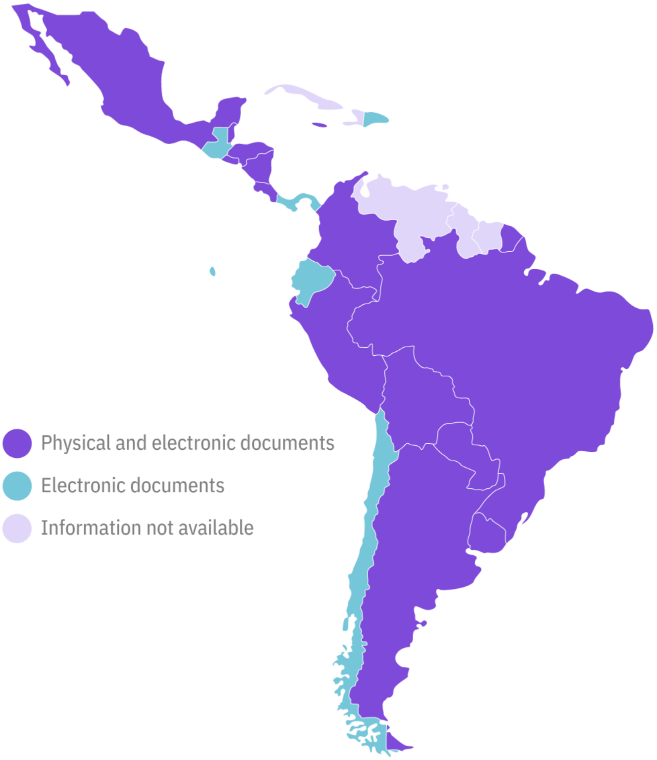


Source: Reprinted from Latin America in the United Nations Electronic Government Index, United Nations (UN), 2018, <*2018 UN E-Government Survey | Multimedia Library - United Nations Department of Economic and Social Affairs*>

Insofar as civil registration and identification are concerned, the development of new solutions and services that facilitate verification and authentication of identification data would not only allow citizens to easily access services, but also facilitate the collection of information to be used to improve government planning and the management of more focused programs and services (IADB, 2019).[11]

Many identification and registration bodies can work online in many Latin American countries, but the use of hard-copy ledgers has not yet been eliminated. In some countries, current legal frameworks require recording vital events in physical books.[12]

Figure 7 : Type of documentary support in civil registries by countr


● Physical and electronic documents
● Electronic documents
● Information not available

Source: Adapted from Civil Registries and Identification Offices: Analysis and Country Records, Inter American Development Bank (IADB), Estefania Calderón, 2019, <*Registros civiles y oficinas de identificación: análisis y fichas de país*>

In Argentina, the national identity document was underpinned by the digital identity system (*Sistema de Identidad Digital,* SID). Uruguay has enhanced its digital government performance considerably, becoming one of the leading countries in this field in Latin America. Since 2007, the country has had a government digitization plan and, as an outcome, it offers digital identity free of charge for all its citizens. In addition, it is expected that by 2020 100 percent of the Uruguayans will have a digital identity. The Peruvian Government recently developed an electronic national identity document (Documento Nacional de Identidad Electrónico, DNI-e), a chip-based card with authentication cryptographic keys embedded.

Despite the negative side of biometric identification use in authoritarian regimes, the Latin American population tends to prefer biometric authentication due to the perceived ease of use (Mastercard, 2019b). Although the report was conducted by a foreign company with commercial purposes, it still provides useful insights into the future development of digital ID in the region.

However, a significant part of the population of Latin America does not yet have access to basic infrastructure, a precondition for the proper implementation of digital ID systems.[13] Low levels of electricity, telecommunications, and data infrastructure augment the digital divide between the rural and the urban areas (Domínguez, 2018), and high illiteracy rates (UNESCO, 2009) are fundamental challenges. The UNESCO (2017) report[14] indicates that more than 200 million Latin Americans remain offline, although Latin American countries have taken significant steps towards digitalization (OECD, 2019a).

1.4. Approach

From the onset of our research project, we sought to understand the situations in which digital ID should be required, how, and by which players. After several rounds of discussions and workshops, it became clear that there was a need to dive deeper into the identification system, the ways it diverges among specific sectors, and how digital identity impacts and is impacted in each sector. Beyond that, we used a risk and human rights lens throughout this process and focused on drawing recommendations to safeguard sustainable digital transformations of identification.

Our overall questions were:

» What are the appropriate uses of digital ID in the sector?

» How can digital ID be used to foster the sustainable development of Latin America?

To answer these questions, during the sectoral use cases analysis process we asked:

» What role does identification play in the sector?

» How does identification take place in the sector, and how does it relate to legal identity?

» What is the diagnosis of the sector in Latin America?

» What are the risks of digital ID in the sector and how can they be mitigated?

» When should digital ID be requested in the sector?

To answer these questions, we split our approach into three stages: (1) An in-depth review of the literature; (2) sectoral use cases analysis; (3) case studies (see Annex I for details). As a note, each case study's analysis will identify both the appropriate use paradigms and risks associated with the case, as well as ways to move forward towards a Good ID scheme.

Section 2

Sectoral uses in the Latin American Context

Photo: Tales Duarte

2. Sectoral Uses in the Latin American Context

2.1. Digital Government Services

Digital Government Services refer to the use of digital technologies as an integrated part of the government's' modernization strategies.[15] The digitization of public services (e.g. tax filing, renewal of credentials, scheduling of appointments, updating personal information, securing authorizations and certifications, among others) is nothing new. It has been keeping pace with the development and maturity of the Internet mostly since the turn of the millennium. At first, it was called electronic government, and it has recently been rebranded as digital government (OECD, 2019d).

To enable the digitization of public services, governments have long invested in digital identity and authentication methods that can ensure easy, secure, and legitimate access to their citizens.

The Role of ID in Digital Government Services

Traditionally, government services have been delivered in person and subject to identification for the practice of certain acts, such as tax filing, driver's license renewal, and for scheduling vaccinations, for example. Due to the digital transformation, digital identity is a key enabler of digital government services. A well-implemented digital identification system that offers a high level of assurance and adopts advanced security features and protocols to protect identities and personal data is paramount to unlock the potential benefits in the sector. These comprise not only saving money and time in the performance of bureaucratic procedures, but also bringing people closer to public decisions, adding security and trust in pursuit of a large participatory process (OECD, 2019c).

Digital identity contributes to facilitating the exercise of citizenship and political involvement, for example by enabling digital consultation channels. A reliable and secure digital identification system is essential to ensure the legitimacy of the consultation process. The same may apply to facilitate direct participation mechanisms, such as referenda, plebiscites, or legislative proposals. For example, the Brazilian App Mudamos allows citizens to petition support for legislative bills by using inviolable digital identities.[16]

Identification Methods and Possibilities for Digital Government Services

Identification for digital government services can vary considerably from country to country. In a given system, a simple single-factor (i.e. login and password) procedure allows users to log into a government platform. In others, users will have to either purchase or be granted a PKI-based token, with which they be allowed multiple procedures, even voting online.[17] Conversely to these centralized systems, digital identification can also be federated, and in a few countries multiple private authenticator providers are available.[18]

A range of credentials could be used to achieve a high level of assurance for authentication and verification, including biometrics, passwords, digital certificates, QR codes, and mobile phones with identity information embedded in the devices.

Contextualizing Digital Government Services in Latin America

Service delivery in Latin America is often designed in a siloed manner, as an isolated initiative of the governmental entity responsible for the provision of the service that focuses on its own internal priorities.[19] In the digital interface, this non-integration is merely reflected, rather than circumvented. This has a negative impact on potential time saving and easiness value for the users and, consequently, user adoption.

In 2015:

73%

OF THE COUNTRIES IN THE REGION HAD ALREADY DEVELOPED NATIONAL DIGITAL DEVELOPMENT STRATEGIES

60%

HAD ALSO ESTABLISHED ONLINE PORTALS FOR SOME GOVERNMENT SERVICES, INCLUDING COLOMBIA, MEXICO, URUGUAY, BRAZIL, AND ARGENTINA. THESE HAVE LED TO RAPID DIGITALIZATION IN THE REGION.

» In part thanks to these initiatives, rapid progress was made in the region’s connectivity (OECD, 2019b).

» Several countries have announced digital government strategies fed by international bodies and consultancy firms, posing lots of potential, but serious concerns.

Risks of Digital Identity in the Sector

- The rationale of digital government is that it must serve the users, and not be an end in itself.[20]
- If each government entity implements its own digital identity an interoperability problem emerges and much of the efficiency and user value potential are lost.
- Digital services can lead to serious risks to an individual's privacy, from leaks and misuse of identification data and various other pieces of sensitive information linked to the user's profile (e.g. income in the case of tax filing).
- Facial identification, in particular, has become a trend in government authentication due to its theoretically greater accuracy. But it could also further entail breaches of privacy and discrimination.[21]
- Data protection regulations are supposed to be first addressed by the government itself, but it is not always the case.
- A "digital first" approach to government services delivery can result in a two-tier set of public services that might exclude or worsen the relationship between government and part of the society, specifically those not able to access or use digital channels so easily (OECD, 2001).
- Digital identification being the key to access these digital services means that a poorly designed national digital ID system may result in a large portion of the population being denied access to the services.

- To mitigate these risks, a multichannel approach for government services delivery is key. This should not be restricted to digital access. In addition, digital identities should be accessible, ideally for free to the user. One must be able to access the entire range of services, regardless of each required level of assurance. This does not mean that PKI-digital certificates should be used for every transaction, rather that users may choose their credentials for specific services accordingly.
- The system should not be implemented just for the hype, without considering what the effective gain for the user will be.

Appropriate Use of Digital ID in the Sector

Digital government services go beyond offering services digitally. They also encompass establishing a relationship through a digital channel between the government and its citizens. On the one hand, the identification requirement for delivering personalized services (digitally or not) is legitimate when a certain level of authentication is a must to confirm the citizen's status, such as for issuing certificates, securing licenses, paying taxes, etc.[22]

On the other hand, identification must not depend on the delivery of citizen-related services regarding access to useful information, transparency of governmental acts, and fostering democracy and citizen engagement, as there is no sense in such a requirement. What matters, therefore, is to critically assess the amount of data required for determining one's identity, the method of authentication[23] used for digital government services, and whether the process is inclusive.

Key Takeaways for an Appropriate use of Digital ID in the Sector

» Digital Government services should encompass, at the very first step, a widely accessible identification system that adds value for the user by simplifying procedures, reducing direct and indirect costs, and enabling transaction services.

» Integrated or federated authentication structures that use shared data from different systems should follow and incorporate robust transparency practices and inform the users about the treatment of their personal data, according to the national data protection law or, in the absence of such law, by following international best practices.

» Digital Government services should reach the most vulnerable groups, so there should be a costless digital identification option for those users. Regardless of the required level of assurance of a given digital government service, the digital credential should be the same and inclusive to users, ideally through costless digital credentials.

Case study: **Chile's Digital Government and Unique Identifier**

Since 1943, the Chilean identification system targets the identification of all residents, instead of only identifying criminals (Laval, 2018). Thereafter, in 1973, the unique number of identity (Rol Único Nacional, RUN) was created, and matches the RUT (Rol Único Tributário), which serves both as civil identification and as a taxpayer identifier. After 1982, the RUT started to be issued at the moment of birth registration and has already been computerized.

Identification is part of the daily life of all Chileans as it is mandatory for almost all formal interactions. As reported by Privacy International, **"if you don't have the RUT (Rol Único Tributário), you can't do it."** (Privacy International, 2018) Therefore, having a RUT is required to access almost all government services.

This means not only providing identification to interact with the state, but also conditioning that interaction to the presence of an identifier. This may lead to statutory exclusion and privacy abuse. For instance, by knowing a person's RUT, through this publicly available information, one can also ascertain their domicile, marital status, some electoral data, and verify the person's full name and of their parents. All this information may be collected legally.

In 2001, online birth and death registration became available. Later, in 2009, a solution for digital authentication named "ClaveÚnica" was launched, it was issued personally through the Civil Registry system. There is an ongoing effort to promote ClaveÚnica as the only way to authenticate for government digital services.

The RUT is required to secure the ClaveÚnica.[24] Moreover, in Chile's recent Digital Government Strategy, digital identity was placed among the six main pillars (Gobierno Digital Chile, 2018). Examples of these digital government service policies include the *Cero Filas* (Zero Queues), which prevents the need of fragmented identity proof in public institutions, and the *Empresa en un día* (Company in one day), which streamlines the process of setting up a company in the country. Nevertheless, roughly half of the public services can be done online, among which less than 15 percent use ClaveÚnica (OECD, 2019e).

Based on that, President Sebastián Piñera stated that *"...public services, in their digital platforms of procedures or services, may only use ClaveÚnica as an instrument of digital identification, for natural persons, replacing any other authentication system of the respective body of the Administration."*[25]

Chile has a personal data protection law (Law 19,628/1999)[26]. As a general principle, it stipulates that personal data may only be processed on the basis of the prior informed written consent of the data subject, with only a few narrow exceptions (e.g. in the case of certain publicly accessible data or purely internal data processing for certain purposes). The law also regulates the rights of data subjects to access, rectification, deletion or blocking and objection in certain cases.

Nevertheless, as pointed out by the Director of Derechos Digitales, the problem in Chile is where digital identification and data protections coincide: There is *"a sense of lack of protection as a general rule"*. Since a person's RUT is not private data, it is possible to get a person's identification number legally.

"As it is possible to build a database with someone's information so easily, and considering it is also simple to transfer this database among private parties, there is a perception that it is not meaningful to store this information, as it is very easy to know. Therefore, there is hardly any opposition to another person collecting it." (Juan Carlos, Director of Research and Public Policy at Derechos Digitales).

The integration of civil registration, civil identification, and digital identity is a positive aspect of the Chilean case. However, there must be clear strategies for accessing basic digital services for those without ClaveÚnica, otherwise it is going to digitally translate into the high centralization aspect of RUT. Moreover, The Chilean ClaveÚnica model can and should be improved to reach privacy and security standards. A possibility is making the registration number private and implementing a platform for personal data oversight along with ClaveÚnica.

2.2. Financial Services (Financial Inclusion)

Considering our research approach aimed to understanding how digital identity can contribute to foster the sustainable development of Latin America, the sectoral use case analysis of financial services focuses on the **financial inclusion** agenda.[27]

Financial inclusion is more than having a bank account. It ultimately means having access to useful and affordable financial products and services that meet the needs of individuals and businesses– transactions, payments, savings, credit, and insurance – delivered in a responsible and sustainable manner.[28]

Digital financial services have scaled up and play a prominent role as a tool for financial inclusion, mainly through mobile money applications implemented in developing nations as a way of leapfrogging conventional banking procedures and streamlining access (Appaya & Varghese, 2019). This is important for the development agenda because it facilitates day-to-day life and helps families and businesses plan for everything from long-term goals to unexpected emergencies. It is also positioned prominently as an enabler of other development goals in the 2030 Sustainable Development Goals.[29]

The Role of ID in Financial Inclusion

For a third of adults in roughly 50 countries with the lowest Human Development Indexes, the lack of documentation is the main reason for not having a bank account (World Bank, 2018b). One of the main reasons argued by financial institutions to condition access to their services to documentation is their obligation regarding compliance with certain internationally standardized procedures, in addition to other regulations within their jurisdictions that require customer identification. For instance, Know-Your-Customer (KYC) and Customer Due Diligence (CDD)[30] are mandatory procedures and fundamental to ensure the institution’s compliance with anti-money laundering rules (AML) and tackling the financing of terrorism (FT).

Digital identification in the financial sector can catalyze multidimensional efforts by financial regulatory bodies and government authorities to simplify the CDD and KYC prerequisites. Moreover, a trusted digital identity could increase the financial institutions’ ability to comply with anti-money laundering (AML) guidelines and tackle the financing of terrorism (FT) (GSMA, 2016).

The financial sector has been the main driver of innovation in identification, authentication, and authorization schemes worldwide. That is likely because the failure to identify someone in a given transaction may lead to direct financial loss. Modern identification management in the sector goes from federated credit card identity architectures in the middle of the last century to open banking nowadays, for example.

From an additional perspective, many international stakeholders (Mastercard, 2019a and McKinsey Global Institute, 2019) have been trying to quantify very optimistic predictions on the economic impacts that a digital identification system could have on the development of the implementing country (Center for Global Development, 2017a) and on financial inclusion and global benefits for the world's most vulnerable (World Bank, 2019a). However, civil society organizations such as Access Now[31] and Privacy International have warned that there is still not enough evidence to support the promised benefits.

Identification Methods and Possibilities for Financial Inclusion

Using account registration within the Brazilian context as an example, the required pieces of information are (i) the number of the identification document and its nature; its issuing entity and issuance date; the names of the person and of their mother; date of birth; citizenship; nationality; the tax payment registry number, and information on whether the person is "politically exposed."

Many entities are transitioning to using legal identity verification through an electronic Know Your Customer. Several financial technology companies are using a mobile-only version of their proof of identity system.

Customer identification is increasingly being made through the verification of uploaded legal identities (e.g. civil identification, passports, driver's license) in a digital platform that may verify, in official government databases, its validity through application programmable interfaces (API). Financial technology companies also rely on documentoscopy algorithms to prevent fraud. For CDD, the procedure it is similar: automated techniques can quickly determine someone's ability to comply with certain rules.

Furthermore, since M-Pesa[32] in Kenya (now used in several African countries), mobile money has been identified as very attractive to new customers, including the unbanked population (Ramada-Sarasola, 2012). In this regard, it is worth noting that in some contexts, such as in Peru, mobile phone numbers persist throughout the users' lifetime. In this case, KYC also relies on the identity verification of a unique state-issued identifier, but it is much simpler to set up an account for basic financial services such as saving money and making payments and transfers.

Finally, a range of emerging technologies is being explored for registration and authentication. Such technologies are at the core of the trending agenda of passwordless authentication by combining multi-factor authentication and biometrics (World Economic Forum, 2020)[33]. With alternative ways[34] of establishing a person's uniqueness, innovation in the financial sector may facilitate cash transfers, remittances, and digital payments, while ensuring financial monitoring, thus contributing to the financial inclusion of the unbanked. Additionally, in the financial sector, distributed ledger technologies are more mature than in any other sector.

Contextualizing Financial Inclusion in Latin America

Several Latin American countries are implementing national strategies for financial inclusion (Villarreal, 2017). **Colombia, Peru and Uruguay are among the countries with the best financial access worldwide.**

13 countries in the region have prepared integrated policies and actions related to distribution, regulation, and education in financial services.

Furthermore, some countries (e.g. Brazil, Chile, Mexico) launched their financial inclusion strategies over a decade ago (Banco Central do Brasil, 2009).

The region is seen as very prominent for the development of the financial technology (fintech) industry and an important market due to the unbanked population demand. Digital banks are becoming increasingly popular. In Latin America, there is an evolving debate on regulatory frameworks, resistance from traditional banks, and cybersecurity issues (Clavijo, S., *et at.* 2019). /, the lack of proof of identity is still a key barrier to the effectiveness of such policies, and little pragmatic attention has been paid to this topic (FATF, 2019).[35]

The Risks of Digital Identity in the Sector

Digital ID alone is not enough to remedy financial exclusion.

» Due to the risk-based profile of the financial sector, KYC processes may end up requiring supplementary biographical, biometric, and historical data from customers.[36]

» Beyond customer and beneficial identification, CDD demands obtaining further information in higher risk situations for determining the nature of financial activities (FAFT, 2014).

» Combined identification and financial data poses great risks for users in case of breaches (e.g. being socioeconomically excluded from specific programs or denied credit) and for the integrity of the financial system (e.g. increased misappropriation of public funds).

» Sharing identification data among financial institutions without clear, informed, and expressed consent from users

» The verification process must be transparent and as costless as possible.

» For basic financial services, there must be simplified KYC processes either physically or digitally, and with privacy by design and by default.

can also be a driver of exclusion and discrimination, hence perpetuating poverty instead of reducing it.[37]

- Charging user identity verification services fees may result in socioeconomic exclusion.

Appropriate Use of Digital ID in the Sector

As mentioned, KYC is a mandatory procedure and user identity verification is a key element for opening bank accounts or for customer and beneficial identification in a given financial transaction. That said, financial entities requesting pay slips to evaluate someone's ability to pay for loans, for example, is expected. However, it is not reasonable to demand and use financial information to determine one's uniqueness.

Furthermore, how user consent for data collection and the sharing of personal data are established in practice is key. For an appropriate use of digital ID in the financial sector, unauthorized access to identity data from third parties must be addressed and publicly communicated.

Key takeaways for an appropriate use of Digital ID in the sector

- Basic KYC requirements must ideally be costless for the target population's financial inclusion and easy to perform. It is important to clearly separate what is the basic data used to identify someone based on the complementary information required for specific services access and customer due diligence.
- As the leading sector in identification from a technological perspective, financial technology companies and large banks should support and be key drivers of privacy-enhancing technologies. In addition, the inexistence of redress and grievance mechanisms to access the history of one's data is an important indicator of bad practice, given the sector's technological maturity.
- Financial regulators should work closely with identification and data protection authorities ensuring interoperability with the national identification system.

Case Study: **Peru and Financial Inclusion**

Peru is a very particular identity case. In 1995, the Peruvian Government started an extensive campaign for identification by establishing, constitutionally, the National Registry of Identification and Civil Status (*Registro Nacional de Identificación y Estado Civil*, RENIEC). As an independent identification authority, RENIEC has overseen the issuing of the National Identity Document (DNI).

RENIEC was created right after a period of civil war, authoritarianism, and persecution that left millions of Peruvians without any proof of legal identity. The autonomous status of RENIEC is ensured by revenue coming from providing identity verification and authentication services to private entities. This accounted for roughly a third of RENIEC's revenue in 2015, and this is likely to increase as nearly the entire population has a DNI, but not necessarily civil registration.

Since 2015, Peru has had a National Strategy for Financial Inclusion that identifies the lack of identity as a key barrier to access (*Comisión Multisectorial de Inclusión Financiera,* 2015). Pagos Digitales Peruanos, a consortium of banks and financial enterprises, launched a mobile payment system called BIM that is often referred to as a case of digital identity-driven financial inclusion (Caruso, 2016)[38]. It is a replication of mobile money systems in Africa.

BIM, a digital wallet, is a non-profit initiative launched in 2011 mainly targeting the unbanked, but only those who own a mobile phone. Unfortunately, this excludes most of the unbanked population who also do not have access to a mobile number (Center for Financial Inclusion, 2019). Approximately 26 million Peruvians have no access to financial services, roughly 80 percent of the population. Nevertheless, both RENIEC and CSO interviewees agree with regard to the failure of BIM in terms of gathering a critical mass of users until now.

DNI is not only required for opening an account. Actually, *"to get a mobile number, you need to use your DNI number"* (Miguel Arce, Sales Manager at Pagos Digitales Peruanos).

The platform's KYC is ensured by the unique identifier code provided by RENIEC and cross-checking in a photo database as part of its economic model.[39] BIM connects with RENIEC and obtains the complementary data associated with the DNI provided by the client when registering in the app. If the data does not match, the account is blocked the following day. The cross-checking is the same for underage or deceased persons. According to an executive in charge of BIM, the only data RENIEC provides in this case is the person's full name and proof of legal age. Once BIM has been installed, the user can choose which financial service provider he or she wants to use.

However, as digital rights advocates argue, the centralized and mighty profile of RENIEC poses serious privacy risks. Unlike RENIEC, the Peruvian Data Protection Authority[40] is not independent. Moreover, there is no clear compatibility between the digital identity and the data protection regulations. Considering all countries in Latin America, in Peru it is particularly easy to access identity photos of citizens.

Regarding RENIEC, ***"from a civil society perspective[41], I do not like that autonomy. An autonomy without control, almost an absolute power."*** (Miguel Morachimo, executive director at Hiperderechos).

Regarding the digital identity legislation, there was no review or consultation for conceiving norms, regulations, programs, applications, whether by the Congress, the Data Protection Authority, the Ministry of Justice, or civil society.

In terms of financial inclusion, even though there is still a huge unbanked population, BIM did not have a significant impact. Nevertheless, the integration between BIM and RENIEC is fair from the perspective of individual usability, convenience of financial service providers, and revenue for the public institution. Meanwhile, from a data governance viewpoint, this integration is worrisome due to the power imbalance of the identification authority over the data protection one. Allowing multisectoral oversight would be a very proactive attitude by RENIEC to strengthen the digital identification system.

2.3. Healthcare

Access to healthcare is established as a human right under the 1948 Universal Declaration of Human Rights as part of the right to an adequate standard of living (art. 25). The right to health is again recognized as a human right in the 1966 International Covenant on Economic, Social and Cultural Rights. Furthermore, SDG 3.9 states the goal of achieving universal health coverage *"including financial risk protection, access to quality essential healthcare services, and access to safe, effective, quality, and affordable essential medicines and vaccines for all."*

The identification of individuals can be a tool to achieve those ends, or conversely, it can wrongly discriminate, preventing access to healthcare by those who are not identified. These potentialities, both good and bad, are scaled up in a digital identification system.

The Role of ID in Healthcare

Identification in the healthcare sector can be valuable for patient security (WHO, 2007), efficiency in health services delivery, and public health management (World Bank, 2018c). Additionally, a patient identifier engine can be important to aggregate records, generate statistics, and organize data to improve health policy planning.

From the perspective of service providers, once the patient's identity is known, it is possible to access relevant treatment and medical history to ensure that consistent and appropriate care is given. From the patient's viewpoint, documentation is important to prove enrollment in insurance programs or other safety nets that cover medical expenses. Regarding the "patient safety" construct, patient identification is one of the most relevant elements presented by international health organizations.[42]

Identification Methods and Possibilities in Healthcare

The emergence of digital identification in the health sector is linked to a proliferation of health information technology policies to implement electronic health services, including electronic medical records, electronic health records, personal health records, and electronic prescriptions – along with expanding initiatives on mobile health (WHO and ITU, 2012).[43]

Current methods for patient identification usually involve the use of a medical record number issued and maintained by the treatment's provider, which does not always have a compatible or an interconnected system. Thus, patients can be linked to several medical record numbers, each issued by the clinic or hospital that provided care to them. The UNAIDS report (UNAIDS,

2014) draws attention to the fact that if used within a broader context, it is virtually impossible, based on the number alone, to determine which patients are the same across organizations or locations. This would undo the benefits described earlier. Additionally, the probabilistic medical record matching method can be another way to identify patients (UNAIDS).[44]

To eliminate the multiple parallel and disconnected patient registration mechanisms, the implementation of a National Health Digital Identifier (NHDID) is often considered. This is a unique number linked to the identification information by the trusted authority. The NHDID issued for a patient usually also includes the issuance of an identifier card. The patient can use the card to communicate their NHDID to other parties who need to use the NHDID information. This process is often accompanied by the request for additional documentation and/or the collection of biometric data.

Contextualizing Healthcare in Latin America

The model for the identification and delivery of health services in a centralized manner in Latin America was built gradually in the 1990s. Previously, healthcare systems had been linked to social security and everyone not linked to that system was directed to a 'general-purpose' service. Those services were later unified in most Latin American countries.

In the previous service delivery model, no information was kept about the patient, except for the procedures performed. Thus, the focus was on documenting and ensuring the correct billing of services, mainly to prevent fraud by the decentralized provider. In the centralized model, meanwhile, both patients and their medical records are monitored to ensure treatment continuity. The change in paradigm required a more sophisticated identification system, which would allow focusing on patient safety.

The progress made by Latin American countries in the field of electronic health services (e-health) is manifold. Data from the region's WHO Member States — made available through its regional office, the Pan American Health Organization (PAHO, 2016) — show a mixed overview of practices related to *e-health*.

77.8 %

HAVE A NATIONAL POLICY OR STRATEGY FOR UNIVERSAL HEALTH COVERAGE.

84.2%

REPORTED HAVING A NATIONAL POLICY OR STRATEGY AT LEAST FOR A HEALTH INFORMATION SYSTEM.

Albeit in a heterogeneous fashion, *e-health* policies and technologies have penetrated Latin American states. A NHDID will likely be the key by which citizens will access those new ways of delivering health services.

2.3.1. Risks of Digital Identity in the Sector

A National Healthcare Digital Identity alone will not protect the privacy and confidentiality of the patient's care information, nor will it ensure its accurate identification.[45]

The digitization of healthcare records and services and the emergence of new technologies raise concerns about privacy (protecting health data, including biometrics) and about the relationship of trust between patients and providers to another level. Thus, the integrity of health data starts turning into a cybersecurity issue.

» Unauthorized access or misuse of personal information can reduce trust, undermine privacy rights, and, in some cases, put vulnerable groups at serious risk of harm (World Bank, 2018c).[46]

» *E-health* systems may become the largest collection of information on a country's citizenry, becoming a *de facto* civil registry. Medical records may reveal ethnic origin or religious affiliation in a systematic manner, which is not appropriate for a general-purpose national identification system.

» Sharing/selling personal data for a variety of dubious purposes, including unethical discrimination by health insurance providers.

» There are groups of people that may be excluded from the healthcare or identification program itself, if this is not planned carefully. Some people, such as immigrants, sex workers, LGBTQ+ individuals, drug users, or those with stigmatized diseases, may be reluctant to identify themselves, and this decision must be fully respected.

» Requesting additional documentation may lead to exclusion. Depending on the country and on the different local

» At-risk groups and those with social stigmas are extremely dependent on the context and culture of each region and, for this reason, specific policies must be designed to include them. For that, it is essential to engage with members of key populations so that potential concerns can be identified and addressed.

» Alternative identification methods may have to be developed to ensure the integrity of the application process for national schemes that require identification, such as vaccination programs. For this, the identification purpose can be achieved by meeting with a village or tribe elder, village or community healthcare worker, religious leader, or other trustworthy source.

» The privacy liability may also be mitigated by enforcing privacy laws and regulations that focus on individual rights while ensuring adequate access to data to meet public health information needs (World Bank, 2018c).[47]

conditions of rural and autochthonous communities, there may be minimal formal documentation to help verify a person's identity. Also, specific situations may prevent part of the population from presenting documents, such as natural disasters, war, or other calamities.

Appropriate Use of Digital ID in the Sector

As mentioned before, access to health services is an internationally recognized human right. In this sense, it is necessary to analyze in detail if and when patient identification is a step towards the realization of those rights or, on the contrary, if it is excluding even more vulnerable groups from access to health. Ultimately, everyone has the right to urgent medical care to save their lives or to avoid irreparable harm to their health, and this should be provided regardless of any identity document being presented.[48]

Key takeaways for an appropriate use of Digital ID in the sector

» If a unique national identification is established for health services, it may be linked to a foundational ID. This link, however, should not allow access to sensitive medical data by third parties. When necessary to meet public health information needs, the data should be anonymized, not allowing the patient to be reidentified.

» Access to urgent medical services, and not just emergencies, should never be conditioned to identification. Hence, that is the case for Digital ID.

» Alternative identification methods may have to be developed to ensure the integrity of the application process for national schemes that require identification (such as vaccination programs). Digital ID may support that.

Case study: **Mexico's Electronic Birth Certificate and Electronic Vaccination Card**

Currently, there are several official documents to identify citizens in Mexico. Among the main ones is the Unique Population Registry Code (CURP). This registration is a combination of letters and numbers assigned by the National Population Council to each person born in Mexico or a foreigner holding a residence permit; however, it has not yet been translated into a universal national ID. Birth certificates and CURP serve as foundational IDs that enable individuals to obtain functional IDs, which are used to vote and to have access to social security programs and public health care services. Although the Coordination of the National Digital Strategy (CEDN), launched in late 2013, recently implemented important electronic health actions, the country does not have a comprehensive national policy or strategy in the field.

Identification is required to receive medical attention in Mexico. This requires attention, as it potentially excludes people who have no means of identification or who do not want to identify themselves to access health services, whether public or private. However, according to the experts interviewed for the scope of this project, people who have no means of identification can receive treatment on an emergency basis by default under the legislation.

Each health system still collects, stores, and processes the data of its beneficiaries. Nevertheless, the government implemented, as part of the National Digital Strategy, the Electronic Birth Certificate (CEN) and the Electronic Vaccination Card (CEV), two new forms of electronic documentation used in the health system.

The CEN is an electronic version of the birth certificate in a unique national format established by the Ministry of Health. This document is issued to newborns by the affiliated health institution of their birthplace.[49] It can have a hardcopy version and will be the first step for a unique digital identity in healthcare.[50]

The electronic version of the birth certificate is not a requirement to obtain a hardcopy of the birth certificate or of the CURP, and the paper version is still in use. Although the General Health Law establishes that it is mandatory since 2015, not all institutions have implemented it yet (Mexico Digital, 2014). According to the Mexican government, the system is already in place in 21 states, and, by 2017, more than 200,000 electronic certificates had been issued (Mexico Digital, 2018). In some cases, the electronic clinical record has already been implemented (Comisión Nacional de Arbitraje Médico, 2018).

The CEV, established in 2014, has the same functionality of the National Health Card that is currently in use, but there is still work to be done to achieve full operationality. Only a few cities have implemented it, and it is only mandatory in the states that have already put the system in place. The project also comprises a mobile application, a control panel, a web administrator, and a vaccination card with a chip. The birth certificate data and the CURP are entered into the chip, and each person's vaccination data is included and stored electronically and backed-up by handwritten data on the same card.

The combination of CEV, CEN, and the electronic clinical records may represent a gain for the government because it would not have to repeat clinical studies several times, since they are already stored electronically. Nevertheless, the Mexican database aggregates sensitive and biometric data of the patient and their families, increasing the damage in case of misuse or leakage. This is worrisome because there are those interested in having access to that database, such as insurance companies.[51]

The Mexican data protection law determines that there must be a legitimate interest for collecting data. However, it does not provide any definition of 'legitimate interest.' Thus, in practice, the current law allows data collection that some consider excessive.

"Compliance with legislation on the protection of personal data held by service companies established in Mexico is minimal, as a result of unfamiliarity with the law." (Enríquez, O. 2018).

In addition, the law does not define the correct data storage standard or consequences for non-compliance.[52] It is appropriate to say that today Mexico has consistent legislation regarding the protection of personal data, but it is still little known and poorly enforced.

Evelyn Tellez, a researcher at INFOTEC (the Government of Mexico's public research center specialized in the development of information and communication technologies), also reinforced certain sensitive issues regarding the storage and processing of personal data by the government. For instance, the data of more than 80 million Mexicans was recently cloned.

In addition, the clinical record is the second most important record in Mexico (the first being the national electoral institute, INE). An explanation for this phenomenon is that in order to obtain a medical appointment, users are required to present proof of address, voter credentials, and a birth certificate for the basic data requirement. On top of that, they are also asked to provide all fingerprints of the user and the user's family (parents and/or children).

There are gaps in the legislation that directly impact the protection of Mexican citizens’ data (OECD, 2018), which becomes evident in analyses of cases of massive leaks of data, as pointed out by Evelyn. Hence, there is a real distrust about the security of data held by the Mexican state[53], and having their identity stolen has been a real issue for Mexicans in recent years.[54] In fact, according to a high-level network and IT solutions provider in Mexico, while credentials such as INE are difficult to counterfeit, the Mexican ID system is still deficient in data security and protection against identity counterfeiting.

2.4. Social Protection

Despite different approaches and definitions, Social Protection is the system of programs, players, policies, and actions to safeguard vulnerable populations, eradicate poverty and promote wellbeing and decent work (UNRISD, 2010). Among the Social Protection Programs (SPP) there are contributory and noncontributory schemes (e.g. conditional and unconditional cash transfers), mainly addressed here.

Considering the holistic approach of the UN's Sustainable Development Goals (SDG), the need for better coordination among social protection programs is in the spotlight.

The Role of ID in Social Protection

Without legal proof of identity, a person cannot be included in hardly any aid program. This is a driver that stimulates the demand for identity documentation among the poor. Studies show that social inclusion drove the demand for civil registration and identification in Latin America (Hunter, W. & Bril, R, 2016; Hunter, 2019).[55] Moreover, governments have created policies to simplify (Muzzi, 2010) identification services and make them more accessible to the undocumented vulnerable population.[56]

The adoption of or linkage to digital identification technologies is an emerging and rapidly increasing trend in social protection programs.

In this sense, an efficient way to identify individuals is essential to ensure interoperability, to link data among programs, to promote social participation, and to improve service delivery.

Identification Methods and Possibilities in Social Protection

Social Protection schemes demand more information about the population than ordinary identification schemes. It is necessary to characterize individuals in multiple aspects of their conditions (e.g. age, income, the number of the householder's dependents). Thus, SPPs adopt a wide range of identification methods that vary according to the capacities of the government, the country's ICT infrastructure, the features of the program, and the target population. In most countries, beneficiary enrollment is done using traditional paper-based foundational IDs.

When the country has a foundational ID system, it is used as a primary source to identify the beneficiaries of social protection schemes. However, when the foundational ID's coverage is not sufficient or does not exist, it is necessary to establish an alternative way to identify the target population. Thus, many countries carry out a specific registration process for the SPP target population and issue a card to identify beneficiaries.

A typical Management Information System (MIS)[57], as the backbone for managing SPPs, has at least three functional pillars:

Enrollment and identification	Targeting and defining eligibility	Enabling transactions and service delivery

The interoperability of registries is combined with the use of a unique identifier scheme to enable a holistic overview of beneficiaries, linking them among various programs. For instance, developing nations have adopted biometric identification because of its potential benefit to ensure accurate identification.

Contextualizing Social Protection in Latin America

Traditional SPPs in Latin America used to be linked to labor policies. As the major innovation in poverty reduction, for over two decades the use of non-contributory cash transfers were the focus in research and policymaking.[58] These SPPs had several commonalities, but differed in their eligibility criteria for poverty situations.

By 2014:

High levels of inequality characterize Latin American societies (Ibarra & Byanyima, 2016). A significant portion of the population is not only poor, but also socially, culturally, and legally excluded. Frequently, those most vulnerable, and, thus, in need of assistance, are also invisible to the state. They are unknown because they do not have any formal personal documentation and, consequently, are not reached by social protection programs.

20

COUNTRIES IN THE REGION HAD A CONDITIONAL CASH TRANSFER POLICY IN PLACE

25%

OF THE POPULATION OF LATIN AMERICA AND THE CARIBBEAN WERE ENROLLED IN A CASH TRANSFER POLICY (ECLAC, 2015)[59]

Risks of Digital Identity in the Sector

Ensuring inclusion in social protection is paramount, but also a complex issue. It involves the identification of individuals who are vulnerable and socially excluded by default, often not only economically, but also in other aspects of their lives.

- Without minimum material conditions and access to information, a person cannot navigate the bureaucratic procedures to have an identity document, let alone a digital identity.
- The vulnerability aspect implies that potential beneficiaries may reside in precarious housing, poorly resilient to the weather, or have no housing at all, being, therefore, often unable to keep their documents. Using biometrics has been widely encouraged to face this challenge.
- Regardless of the growing adoption of biometric identification (Carmona, 2019), studies conducted in the Indian context[60] show that the risk of excluding vulnerable groups is considerable (Drèze *et al.*, 2017; Muralidharan, 2020).[61]
- Identification in SPPs collects a wide range of personal data. This means that many sensitive data are exposed to the risks common to any digital identification scheme, such as leakage, but that specifically in the context of social protection can mean stigmatization and embarrassment.
- Digital divide (including digital literacy and technology and Internet access) is often intrinsic to the situation of vulnerability of those who depend on social assistance, entailing a high risk of exclusion.
- Any system failure poses great risks of exclusion and may lead to serious consequences. For instance, if a person does not have the digital identity mandated by government agencies or if his or her digital identity is "incomplete" because their fingerprints are not uploaded to the national database due to poor Internet connectivity (Access Now, 2018).

- This tricky situation has been faced by creating social protection programs that simultaneously address both sides of the equation: Providing minimum income and access to basic services and simplifying the procedures to get basic personal documentation.
- In this sense, data protection must be perceived as an element of social protection (Sepúlveda, 2019).
- In this regard, Social Protection identifiers should not be linked to biometric databases.

Appropriate Use of Digital ID in the Sector

In the social protection context, the identification of beneficiaries is an essential and integrated component of the scheme. Making individuals eligible for social protection is a way to include them. However, there are concerns about the means used for identification.

In Latin America, the adoption of mandatory biometric identification is not yet widespread. However, criticism about fraud has been putting pressure on the adoption of biometrics in social protection programs. It should be carefully considered with a public risk assessment, and biometric data should not be mandatory for individual authentication for access to goods and services.

Key takeaways for an appropriate use of Digital ID in the sector

» Governments should create a single registry for social protection, adopting an inclusive perspective to improve the capacity to reach the vulnerable population. It is crucial to simplify and to make identification services more accessible for the undocumented population by balancing requirements and the conditions of beneficiaries.

» The integration of Management Information Systems and digital identification schemes must take into consideration the risk of excluding the most vulnerable population, while targeting policy effectiveness.

» The adoption of biometric technology in social protection needs to be preceded by a holistic assessment of the national identification system, in which institutional and legal frameworks should be evaluated through the lenses of inclusion and the promotion of rights, ensuring that the poor and most vulnerable are not excluded.

Case study: **Brazil's Unified Registry for Social Programs**

The Unified Registry for Social Programs (CadÚnico) is an administrative record developed in 2001 to support integrated social programs in Brazil, supporting several social protection programs, such as the Bolsa Família (PBF) conditional cash transfer program (Lindert *et al.*, 2007; Hellmann, 2015).

CadÚnico is the beneficiary identification tool, and it differentiates the needs of target populations according to the characteristics of each family. The registration process is free of charge and decentralized within the three federative levels of government. It is used for enrollment and to collect information on the most vulnerable families, including work conditions, family composition, and housing, among others. More than 13 million households in all regions of the country, nearly a quarter of the Brazilian population, have been included in the program.

The Unified Registry also played a significant role in creating demand for birth registration and civil identification. Thus, it helps to make invisible populations eligible for social protection measures. Being an undocumented person in Brazil means being a second-class citizen, perhaps even worse: A person holding no identification document can feel dehumanized.

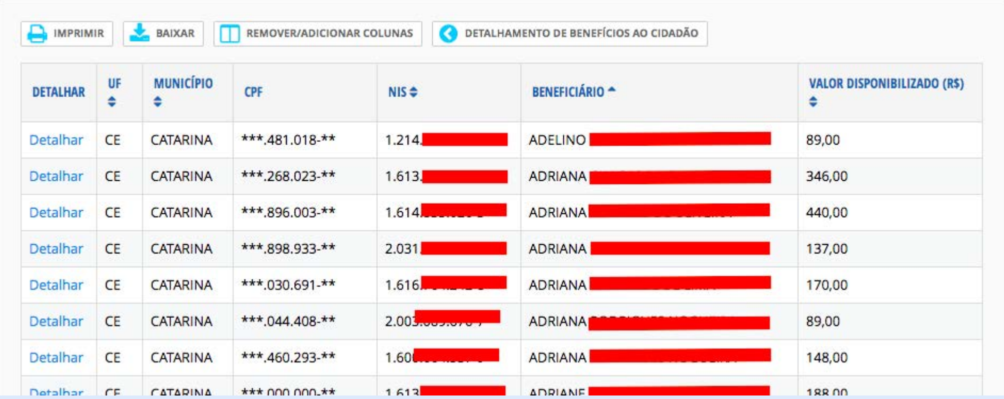
By law, access to essential public services is free of charge for underprivileged persons, but the complexity of the identity ecosystem imposes restrictions on individuals. This is the case because the regulation of services requires the presentation of documents, as highlighted by Raquel Chrispino, a judge in Rio de Janeiro:

'There are Brazilian rules that impose administrative routines, so we are talking about Ordinances, Resolutions, we are talking about normative administrative acts that, in order to regulate the public service, end up forcing citizens to enter some of their ID numbers into a certain system.' (Chrispino, 2019).

Historically, the enrollment processes for the most excluded groups are different from those for the general population. Even undocumented individuals are included in the record, and they receive instructions for issuing birth registration and identification (Brazil's Ministry of Social Development, 2015).

Most PBF recipients are women and black or mixed-race individuals. The analysis of the family composition of PBF recipients reveals that female headed single-parent households represent the largest group (Campello & Neri, 2014). Qualitative research shows that the inclusion of women in Bolsa Família creates and expands opportunities for the personal freedoms of individuals, opening more possibilities for empowering women generally (Campello & Neri, 2014). The essential role of personal documents for citizen empowerment and access to services is clear.

Despite the global recognition of the conditional cash transfer program and its Management Information System, enrollment in the program occurs under the precondition that beneficiaries will have their data fully displayed in the government transparency portal. Even though the Brazilian Data Protection regulation determines the need for expressed and informed consent[62], sensitive data is still displayed under forced consent, as it is a condition for accessing the PBF.

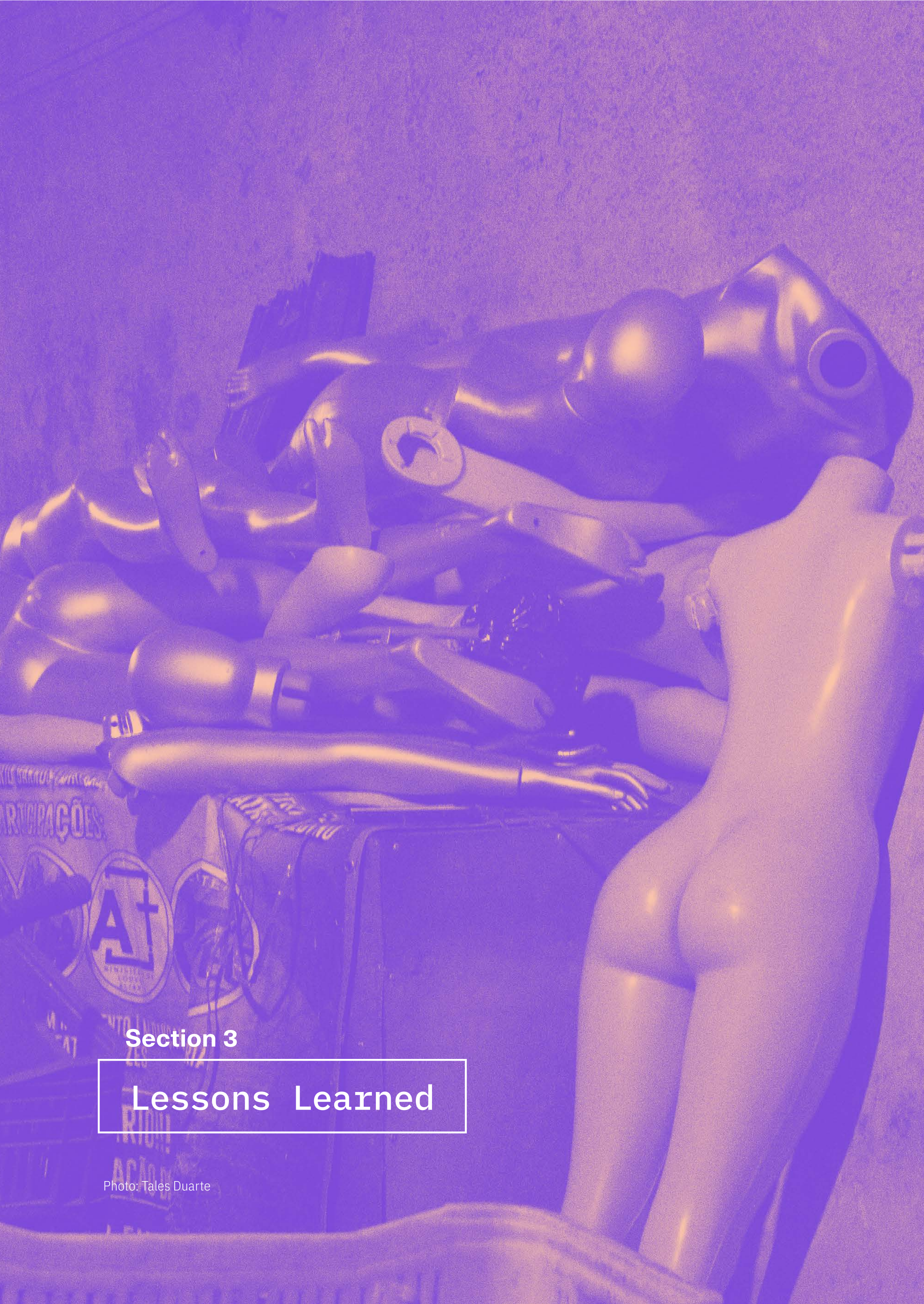

IMPRIMIR
BAIXAR
REMOVER/ADICIONAR COLUNAS
DETALHAMENTO DE BENEFÍCIOS AO CIDADÃO

DETALHAR	UF	MUNICÍPIO	CPF	NIS	BENEFICIÁRIO	VALOR DISPONIBILIZADO (R$)
Detalhar	CE	CATARINA	***.481.018-**	1.214[redacted]	ADELINO [redacted]	89,00
Detalhar	CE	CATARINA	***.268.023-**	1.613[redacted]	ADRIANA [redacted]	346,00
Detalhar	CE	CATARINA	***.896.003-**	1.614[redacted]	ADRIANA [redacted]	440,00
Detalhar	CE	CATARINA	***.898.933-**	2.031[redacted]	ADRIANA [redacted]	137,00
Detalhar	CE	CATARINA	***.030.691-**	1.616[redacted]	ADRIANA [redacted]	170,00
Detalhar	CE	CATARINA	***.044.408-**	2.003[redacted]	ADRIANA [redacted]	89,00
Detalhar	CE	CATARINA	***.460.293-**	1.60[redacted]	ADRIANA [redacted]	148,00
Detalhar	CE	CATARINA	***.000.000-**	1.613[redacted]	ADRIANE [redacted]	188,00

Source: Reprinted from Transparency Portal with full information on beneficiaries, Brazilian Federal Government <www.transparencia.gov.br>.

A positive aspect is that the social protection program identifier is not directly linked to a biometrics database. If the government is intending to implement it, this must be done with a clear and broad risk assessment, explicit mentions to data protection safeguards, and by means of public consultations.[63]

Finally, a key point is the use of the taxpayer number as the main identifier in Brazil, as it is requested not only to the head of the household, but to all his or her dependents. The taxpayer identifier is not civil identification, and irregularities in electoral or fiscal duties have led to the exclusion of those who need it the most. This requirement must be reconsidered for social protection programs, or there must be an overall restructuring of the identification system.



Section 3

Lessons Learned

Photo: Tales Duarte

Lessons Learned

Identity touches the very core of human dignity. Identification is a matter that dates back much longer than digital transformation and data governance agendas. However, its complexity is still barely understood by policymakers. This facet is often overlooked and digital identification systems are deployed focusing primarily on government-centered objectives, as opposed to a user-centered approach, repeating what happened in the computerization of government databases in the second half of the last century.

What are the appropriate uses of digital ID?

There are several key insights that emerged during the research associated with this report. In addition to those already highlighted along the sectoral use cases, this section presents four sets of recommendations designed for policymakers and other stakeholders that ultimately emphasize that the use of digital ID can only be appropriate when it is a tool that facilitates access to rights and services by the user. In addition, this section also highlights that these objectives cannot be achieved when the digital identification system does not guarantee inclusion, user value, privacy and security, because it can mean an additional barrier - enhancing exclusion - or a means to wrongly discriminate. These parameters and their subsequent recommendations are as follows:

1. Inclusion: Digital identification can only be considered appropriate when it promotes inclusion.

» **Beware to not reproduce the current exclusion problem digitally.** In all the country case studies, identification is mandatory, whether legally or de facto, for the full enjoyment of rights and services. The exclusion from accessing basic services due to lack of identification may be an analog problem that should not be transposed or enhanced digitally. Chile and Peru's main identification documents (RUT and DNI, respectively) are essential for individuals to perform necessary and everyday actions. However, securing the Clave Única, the Chilean key to government digital services, is not possible without the RUT. The Peruvian initiative for financial inclusion (the main barrier of which is the lack of means of identification) addresses only those who own a mobile number, but to get a mobile number one needs a DNI number. Mexico seems to be following the same path, since most private and public procedures cannot be performed without official identification, and digital identification has also been gradually required.

- **Access to basic rights and services should not depend on digital identification.** As noted, identification, whatever the format, cannot be a barrier to access basic services and rights. Consequently, nor can digital identification. Hence, understanding and considering inequality in access to the ICT infrastructure and the digital literacy divide context is essential when implementing such a system. Many Latin American countries are still struggling with inequality in access to technology and digital illiteracy. Thus, any agenda that establishes digital identification as the only access route is exclusionary by design. Multichannel access is a must in the region.

2. User Value: Balance Individual and Institutional Interest.

- **Making sure that digital identification schemes are leveraging people's rights, not underpinning their civil liberties and rights.** Insofar as sectoral uses are concerned, the fine line between identification as a right or as a means of intrusion, surveillance, and an increased factor for the power imbalance between institutions and individuals in a foundational identification system is reflected and, therefore, the identification system must clearly articulate its intended uses, both in the immediate term as well as in future scenarios. This also means that a deployment framework addressing data minimization, clear purpose, and other necessary guardrails to protect users against potential abuses is paramount.
- **Do not join the hype at the expense of effective user value.** Adopting flashy technology, regardless of its appropriateness for the given context, shows a predominant interest of the institution in appearing modern rather than addressing its users' actual needs. For instance, some sectoral uses of digital identity within digital government proposals appear to be mainly political branding, as in reality most services offered cannot be 100 percent digitally achievable or, even worse, they may contribute to increasing the digital and services access divide.
- **When innovation brings real value to the user and inclusion, go for it.** In certain contexts and use sectors, digital identification can add real value to the user and contribute to inclusion. For instance, it was observed that in the sectoral uses of financial inclusion and social protection, DID provided alternative ways of establishing a person's uniqueness, leapfrogging the given barriers. In the former, the technology contributed

to facilitate cash transfers, remittances, and digital payments, while ensuring financial monitoring, thus contributing to the financial inclusion of the unbanked. In the latter, it did facilitate enrollment in the assistance program and, outside the Latin American case studies, the granting of benefits in real-time base updates has also been documented. For instance, Indian identification system users (Aadhaar) stated that biometric identification increased their control over their finances and ensured regular payments (Gelb, A. et. Al., 2017).

3. Privacy: Prioritize data protection laws that safeguard the privacy of personal data.

» Have in place an appropriate and comprehensive regulatory framework. All four case study countries have a data protection law in place.[64]However, as the case studies in this report have shown, the legal data protection framework must be appropriate and comprehensive. Mexico's data protection law lacks clarity. For instance, the imprecise concept of legitimate interest (authorizing the collection of personal data without the consent of the data subject), hampers assessing the adequacy of data collection and, consequently, excessive collection, even from family members, is a common practice in the country. In Chile, the current legislation allows any individual to legally access a large portion of personal data derived from the Chilean identification number (RUT), which is legally considered public information.

» Make sure the legislation is widely known and enforced. The Mexico and Peru cases illustrate how the lack of discussion and publicization of the relevant legislation among stakeholders also minimizes the effectiveness of legally recognized rights. In the Mexican case, one of the barriers to complying with the legislation is its lack of awareness and accountability mechanisms, whereas in Peru there is resistance due to perceived authoritarian ways of conceiving and imposing such legislation. In Chile, personal data protection legislation does not adequately protect data privacy - by not protecting the RUT number with a private status, several other data are legally accessible by anyone, significantly compromising the users' privacy.

4. Security: Take a comprehensive look at security and privacy by design.

» Ensure robust mechanisms for safeguarding user data privacy and integrity. Without a robust, adequate, and secure technological design that ensures the system's ability to secure user data, digital identity should not be implemented. The case studies explicitly show how the individual's data are currently extremely exposed. For instance, there is an important record of identity data leakage under Mexican government's auspices. The fact that health and financial data required in sectoral uses of digital identification are very sensitive, and that their misuse or leakage can lead to exclusion and discrimination should not be overlooked. To name just a few risks, the exposure of a disease status or an economic vulnerability situation can mean being denied credit or facing higher health insurance rates, hence perpetuating poverty and service exclusion instead of reducing it, not to mention how these can also be a driver for social exclusion and discrimination.

» **The collection of sensitive data should be minimized.** There are different minimal data sets regarding specific sector purposes. However, most of them collect more data for registration than needed for their original purpose. This compromises security because the amount of data collected is proportional to the risk of mission creep and the potential damage to user privacy in the event of data leakage, misuse, or unauthorized sharing. The Mexico case illustrates unjustified requirements for data to be added to the users' clinical records, such as voter credentials and fingerprints, both of the user and of their family members.

Annex I: Research Stages

In the first stage, we conducted a solid review of the literature concerning identity management from a chronological, geographical, and multisectoral perspective. The main sources for research were journals, books, websites, and articles. Among them, it is relevant to highlight the following: Identification Revolution: Can Digital ID be Harnessed for Development? (Gelb & Metz, 2018); OECD Digital Government Reviews[65]; Access Now's assessment on National Digital Identities (2018)[66]; ITU's Roadmap for Digital Identity (2018)[67]; World Bank ID4D collection with a focus on the Practitioner's Guide (2019)[68] and country diagnostics; and McKinsey's report entitled Digital Identification: A key do inclusive growth (2019)[69]. We also conducted specific bibliographic research on sectoral uses. Additionally, we assessed historic identification documents of Latin America to gain a better understanding of the regional scenario.

In the second stage, we analyzed the sectoral use cases. We focused on digital government services, financial inclusion, healthcare, and social protection. This choice was made because these sectors could provide a relevant overview of digital ID in terms of fundamental rights (healthcare and social protection) and emerging services (digital government and financial inclusion). Each of the sectoral use cases were accompanied by a case study.

In the third stage, we conducted country-specific analyses and a series of interviews in each country. The case study choices were based on the current discussion and available data on those sectoral uses in specific Latin countries. We found that it would be appropriate to focus on Mexico for healthcare given its electronic vaccination record; on Peru for financial inclusion due to it often being seen a benchmark for digital ID-led mobile wallets; on Chile for its digital government services that have an integrated approach to identification and an advanced digital government agenda, and, finally, on Brazil for social protection, since its conditional cash transfer program and its management information system are globally recognized.

Notes

1. An identity established within a system meant to be used by other entities. States often operate foundational ID systems through Civil Registration and Vital Statistics (CRVS) agencies with centralized databases. India's Aadhaar and the Social Security Number in the United States are examples of foundational IDs, and in some cases birth certificates, passports, and other government-issued credentials are used as foundational IDs.

2. In addition to the potential benefits described, organizations draw attention both to the inherent risks of Digital ID systems and to the challenges and opportunities more specific to the context of the Global South countries.

3. For more on the Good ID movement, go to https://www.good-id.org/en/about

4. Aadhaar, in India, and the e-ID, in Estonia, are two common examples of foundational digital identities.

5. Child marriage levels in the region have remained around 25 percent in the past decade, while other areas of the world have seen significant declines, particularly in South Asia, where child marriage levels have dropped from almost 50 percent to 30 percent in the same period. For more details, go to <https://www.unicef.org/press-releases/latin-america-and-caribbean-decade-lost-ending-child-marriage>

6. The issue of the system's ease of use should consider the users' digital literacy levels, language, and age.

7. Diversely, it was a method to identify individuals in their civil relationships with the State and with other individuals.

8. The original remark, in Spanish, was: *"La Identificación de todos los habitantes sin distinción, para garantizar, como lo he dicho, el derecho al nombre y contribuir eficaz y seguramente a que sea verdad el buen funcionamiento de las instituciones del Estado, para bien de la sociedad por ellas regida."*

9. The index is composed of three factors: Online services index, telecommunications index, and human capital index.

10. Most Latin American countries score between 0.45 and 0.65.$

11. Although the use of technological tools drives the improvement of service quality, it is also necessary to have clear and standardized procedures, in addition to a multipurpose digital identification so that the user can carry out the process in an agile, efficient manner.

12. A study carried out by the Inter-American Development Bank (IADB) shows that among the 20 countries that provide civil registration services, 14 must keep hardcopies of birth certificates or digitally processed certificates (IADB, 2019).

13. For instance, in 2016 the World Bank estimated that a significant part of the population, mostly in rural areas, still does not have access to electricity. Retrieved from <World Bank, Sustainable Energy for All (SE4ALL) database from the SE4ALL Global Tracking Framework led jointly by the World Bank, International Energy Agency, and the Energy Sector Management Assistance Program. https://data.worldbank.org/indicator/EG.ELC.ACCS.ZS?view=map>

14. Sociedad digital: brechas y retos para la inclusión digital en América Latina y el Caribe. Published in 2017 by the United Nations Educational, Scientific and Cultural Organization (7, place de Fontenoy, 75352 París 07 SP, Francia) – UNESCO and the Regional Bureau for Sciences in Latin America and the Caribbean, UNESCO Montevideo Office (Luis Piera 1992, Piso 2, 11200 Montevideo, Uruguay).

15. The term is used as a sectoral use of digital identity by the World Bank's Identification for Development (ID4D) literature.

16. "Mudamos" is a mobile app that allows people to support citizen initiatives draft bill in Brazil through electronic signatures. By making use of the constitutional mechanism of direct democracy and ensuring the levels of assurance of inviolable digital identity, it has facilitated civic engagement in several cities' legislative houses. See more in: <https://www.mudamos.org/>.

17. Several governments are experimenting novel approaches, including blockchain-based identities; for instance, this is among the core use cases in the European Blockchain Services Infrastructure. See <https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=147458240>

18. The United Kingdom adopts an identity assurance system that is intended to provide a single trusted login across all UK government digital services. See <https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify>.

19. As an example, the Brazilian public administrative records and identification system is very fragmented. This has led to the increasing adoption of the taxpayer number as the major identifier in the country. See <http://mapadainformacao.com.br/>.

20. For instance, when the digital government proposal is mainly a political branding, but in reality most services offered are not 100 percent digitally achievable.

21. An example of this trend is the Commonwealth's my GovID, which is being tested in Australia this year with a facial recognition feature. See <https://www.mygovid.gov.au/>. On the other hand, empirical evidence has shown the existence of algorithm bias in such technology, leading to age, race, and ethnicity discrimination, hence raising concerns in its premature stage for massive adoption. See <https://www.theverge.com/2019/12/20/21031255/facial-recognition-algorithm-bias-gender-race-age-federal-nest-investigation-analysis-amazon>

22. It is important to emphasize that the form of digital identification required must guarantee the security and privacy of the user and, as a case of public utility, such required digital identity must be accessible to everyone who wants to use it, which means that it should be free of charge and discrimination, and ease to secure.

23. When considering authentication methods, the United Kingdom's identification system can serve as an example, since it uses different levels of identity assurance instead of a single "gold-standard" identity required to access government services online. The identity assurance framework and the standards developed for determining what forms of identity evidence meet each level of identity assurance provide valuable guidance for other countries and can be easily adapted to different contexts (Whitley, 2018).

24. One must go to the Civil Registry and Identification offices with the identity card, provide an e-mail, register on the website, and validate with RUN.

25. In the presidential instruction on digital transformation. See more in <https://digital.gob.cl/instructivo/acerca-de>.

26. https://www.leychile.cl/Navegar?idNorma=141599

27. See: <https://www.uncdf.org/financial-inclusion-and-the-sdgs>.

28. According to the World Bank, quality of life can be improved with access to financial services, this considering the potential investments, risk management, and insurance. See <https://www.worldbank.org/en/topic/financialinclusion/overview>.

29. What differs is the dataset required. Financial inclusion programs tend to request an identification number and a phone contact, while traditional banks request information on someone's financial background – biographic, biometric, supporting evidence, and metadata.

30. At the core of CDD, as a subset of KYC, is the process of ensuring one's identification, verification, and ability to comply with certain rules in the financial sector. This is intended for monitoring and understanding the nature of transactions.

31. See more in <https://www.accessnow.org/whyid-letter/> and <https://privacyinternational.org/long-read/2237/sustainable-development-goals-identity-and-privacy-does-their-implementation-risk>.

32. Launched in 2007 using SMS for cash transfers, M-PESA is the most notorious case of mobile money. It was an outcome of a major telecommunications company of the country (Safaricom) and a foreign one (Vodafone). Following that episode, the telecommunications sector has developed mobile-based digital wallets worldwide.

33. Regarding passwordless authentication, concepts such as Zero-Knowledge Proof and Proof Bullets also are at the core of blockchain-based digital identity. It allows, for example, a person to know if another is compliant with specific rules without him or her disclosing that information.

34. Several digital banks rely on image recognition of official documents, video records, and even live streaming for proof of identity.

35. In this regard, the Financial Action Task Force (FATF) launched a consultation draft in late 2019 identifying the relevance of digital ID in ensuring efficiency, reliability, security, and inclusion.

36. The KYC procedure demands identifying and collecting a series of customer data from one or more financial services, as well as ensuring certain characteristics about them, based on principles like timeliness: The ability to perform all the risk mitigation procedures in a given and sufficient period of time for a decision to be made. Truthfulness: The ability to utter the truth (considering that misleading information and some omissions are morally equivalent to lies), and integrity.

37. With the growth of digital financial services, consent is becoming a central topic to digital identity in the sector (Loufield and Vashish, 2020).

38. The system is enabled by a simplified way of establishing a KYC through identity validation by a central state authority for a specific Electronic Money Law, regulating the basic features of electronic money as a financial inclusion instrument. *Ley del Dinero Electrónico* 2013 (Peru). See more in <https://www.bcrp.gob.pe/docs/Transparencia/Normas-Legales/ley-29985.pdfl>.

39. BIM's representative argued that even though they want to go fully digital in 2020 and use biometrics, the cost for accessing RENIEC's database is comparatively higher than in other countries, even for opening bank accounts. An equivalent of 50 cents of Peruvian Soles per person, which can be costly if considering a scenario of hundreds of thousands wallets being opened every day.

40. Since 2011, Peru has had a personal data protection law and a National Authority for Personal Data Protection (Autoridad Nacional de Protección de Datos Personales, ANPDP). However, it is not an independent body and functions under the auspices of the Ministry of Women and Justice. In accordance with Article 7 of the Organic Law of RENIEC, the entity is responsible for "ensuring the privacy of personal data." Even though the DPA has been in place for almost ten years, they deeply rely on RENIEC to ensure data protection. See <http://www.minedu.gob.pe/otd/pdf/normas/01-ley-26497-ley-organica-del-reniec.pdf>

41. He manifested this by highlighting that RENIEC oversees complying with their own norms and that it has not implemented mechanisms to enable participation and revision mechanisms. Some privacy advocates assert that the identification authority's employees support the idea of the "culture of secrecy."

42. Patient misidentification was cited in more than 100 individual root cause analyses by the United States Department of Veterans Affairs (VA) National Center for Patient Safety from January 2000 to March 2003. Source: Mannos D. NCPS patient misidentification study: a summary of root cause analyses. VA NCPS Topics in Patient Safety. Washington, DC, United States Department of Veterans Affairs, June–July 2003 (http://www.va.gov/ncps/TIPS/Docs/TIPS_Jul03.doc, accessed on 11 June 2006) + World Alliance for Patient Safety (2004, WHO); Nine Patient Safety Solutions (2007, WHO).

43. Electronic health services (eHealth) can also be understood as the use of the Internet and other related technologies in the health industry to improve access, efficiency, effectiveness, and the quality of the clinical and business processes used by health organizations, physicians, patients, and consumers, with the ultimate goal of improving the health status of patients. See Eysenbach G. What is e-health? J Med Internet Res 2001;3(2):E20.

44. The matching process must be linked to the patient indexing system and may require significant computational power, a widely available communication infrastructure, and considerable resources to implement it online. Also, the use of algorithms is subject to accuracy problems and precision considerations.

45. That depends on security measures, such as role-based access security, secure communications, and appropriate technology infrastructure. Furthermore, proper controls on access to information on healthcare websites are also required.

46. While those concerns are true for any identification system, they escalate in the health context, particularly if unique identifiers are linked to health records or other potentially sensitive data.

47. For example, sensitive data should be anonymized, preventing the patient from being reidentified.

48. This is a recommendation recognized in several international documents, such as the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (art. 28) and the Special Rapporteur on Health of the UN OHCHR.

49. It is generated by the Established Electronic System (e-SINAC). According to the Mexican government, the system has already been implemented in 21 states, and by 2017 more than 200 thousand electronic certificates had been issued. See more in: <https://www.gob.mx/mexicodigital/articulos/certificado-electronico-de-nacimiento-142911>.

50. See more in: <https://www.gob.mx/mexicodigital/articulos/certificado-electronico-de-nacimiento>.

51. As manifested by an interviewee, there is an issue regarding clandestine traffic of identity data and there have even been massive leaks of data in possession of the National Electoral Institute (Instituto Nacional Electoral, INE), which have made the control people have over their identity problematic.

52. Compared to the GDPR, which has a clear penalty of 4% of a company's annual revenue as a non-compliance fine.

53. In 2015, a database containing voter registration records was published online, exposing the personal information of 93.4 million Mexican citizens. In 2016, a major leak of data from car hire app Uber took place. In October 2017, it was revealed that MoneyBack, the company responsible for returning value-added tax to foreign tourists who visited Mexico, left an unsecured database on the internet with 400 GB of files of sensitive personal information, such as passport numbers, credit cards and official IDs of foreign citizens. See more in: <https://privacyinternational.org/state-privacy/1006/state-privacy-mexico>.

54. In 2016, the Bank of Mexico estimated the value of fraud linked to identity theft at 108 million pesos, which puts the country in eighth position in the world in this type of crime. In 2017, bank card fraud, identity theft and unauthorized access or misuse of personal information were the main concerns of Mexican consumers, according to the most recent Unisys Security Index. See more in: <https://mundocontact.com/preocupa-a-mexicanos-robo-de-identidad/>; <https://mundocontact.com/robo-de-identidad-y-fraude-bancario-angustia-a-mexicanos/>.

55. It is not possible to claim that there is a causality between poverty reduction and access to personal documentation, but we can assert that strategies that combined these two elements created conducive conditions to improve both issues.

56. The continent has been achieving valuable results. In twenty years, Latin American countries accomplished significant progress regarding birth registration coverage. In 2000, the continent had 76 percent of coverage for children under five, and, now, according to a recent UNICEF report, that percentage has grown to 94 percent. See <https://www.unicef.org/reports/birth-registration-every-child-2030>.

57. A Management Information System is the set of technologies, processes, and players involved in the information management for social policies and programmes. A MIS plays a crucial role in Social Protection. It has functions such as promoting outreach to beneficiaries to include them, and multiple administrative functions, such as providing managerial information, integrating and controlling information, and providing transparency.

58. Some examples are Chile Solidario, Prospera (Mexico), Mas Familias in Acción (Colombia), Juntos (Peru).

59. That said, some beneficiaries are still in vulnerable situations (UNU-WIDER, 2016).

60. The Aadhaar case is emblematic because it collected biometric data of over one billion people, hence providing unique digital identification to nearly all the population. Nonetheless, there are some cases of food rations being denied due to system authentication failures and to the discrimination of marginalized groups. See <https://www.hrw.org/news/2018/01/13/india-identification-project-threatens-rights>.

61. Biometrics can make people *"feel watched and tracked and tagged and profiled, and that will have consequences for the way in which they constitute their politics and its expression. The vulnerability of poverty exacerbates this threat to freedom. Of course, there will be someone somewhere who will say that the poor have no use for freedom,"*, as highlighted by Ramanathan (2014).

62. The Ministry in charge also makes available deidentified databases for research purposes online. However, the government should clarify how they prevent re-identification from data inferences.

63. Additional data protection concerns arise with the executive ordinances of creating a unified data registry aiming at interoperability among government databases, but without publicizing, if any, the data risk assessment and engaging with civil society. CSO were surprised with the measure. See <http://www.in.gov.br/en/web/dou/-/decreto-n-10.046-de-9-de-outubro-de-2019-221056841>

64. Brazilian data protection legislation was passed in 2018, but the effects of many of its provisions, notably enforcement and applicable sanctions, which were due to take effect in January 2020, have been postponed to 2021.

65. he OECD has a set of country diagnostics of digital government that classifies a digital identity framework as a foundational element. In this project, we mainly used the reviews of Brazil, Mexico, Peru, and Chile. The information was retrieved from <http://www.oecd.org/gov/digital-government/>.

66. Access Now analyzed, as a third-sector representative, a few specific national digital identities and delivered specific recommendations on the use of biometric data. Document retrieved from <https://www.accessnow.org/national-digital-identity-programmes-whats-next/>.

67. The International Telecommunications Union (ITU) roadmap on digital identity guide provides the diagnostics of the countries and recommendations on best practices and standards. Retrieved from <https://www.itu.int/pub/D-STR-DIGITAL.01-2018>.

68. Launched officially in mid-2019, this report is an extended guideline for decision makers and operations professionals to develop a digital identity strategy, bearing in mind the status quo of the given context, its particularities, the set of policy, design and technology options, and implications. Retrieved from <http://documents.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-Guide-Draft-for-Consultation.pdf>.

69. The McKinsey Global Institute launched, in the first half of 2019, an extended report that also examined different sources of value creation through the use of Digital Identification. It highlighted the huge potential of GDP increase until 2030, both in developed (3%) and developing (6%) nations, on average. Retrieved from <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth>.

Literature

Aadil, A., Gelb, A., Giri, A., Mukherjee, A., Navis, K., Thapliyal, M. (2018). Digital Governance: Is Krishna a Glimpse of the Future?. Center for Global Development Notes. Retrieved from <https://www.cgdev.org/sites/default/files/digital-governance-krishna-glimpse-future-working-paper.pdf>.

Access Now. (2018). National Digital Identity Programmes: What's next?. Retrieved from: <https://www.accessnow.org/cms/assets/uploads/2018/06/Digital-Identity-Paper-2018-05.pdf>.

ACP. (2019). Extreme poverty and digital welfare: New report from UN Special Rapporteur on extreme poverty raises alarm about the rise of a digital welfare dystopia. Retrieved 30 March, from: <https://www.apc.org/en/news/extreme-poverty-and-digital-welfare-new-report-un-special-rapporteur-extreme-poverty-raises>.

Appaya, S., Varghese, M. (2019). Digital ID – a critical enabler for financial inclusion. Retrieved 28 March, from: <https://blogs.worldbank.org/psd/digital-id-critical-enabler-financial-inclusion>.

Banco Central do Brasil. (2009). Perspectivas e desafios para inclusão financeira no Brasil: visão de diferentes atores. Brasília. Retrieved from: <https://www.bcb.gov.br/Nor/Deorf/projincfin/livro_inclusao_financeira_internet.pdf>.

Baya, V. (2019). Digital Identity: Moving to a decentralized future. Retrieved 30 March, from: <https://www.citi.com/ventures/perspectives/opinion/digital-identity.html>.

Barca, V., Makin, P & Bamezai, A. (2018). Integrating digital identity into social protection. An Analysis of potential benefits and risks. Discussion Paper. Oxford Policy Management.

Bhadra, S. (2019). Five Surprisingly Consequential Decisions Governments Make About Digital Identity. Retrieved 30 Msfrom: <https://www.omidyar.com/blog/five-surprisingly-consequential-decisions-governments-make-about-digital-identity>

Centre of Excellence for CRVS Systems. (2020). Gender Equality. Retrieved 30 May from: <https://crvssystems.ca/gender-equality>.

Center for Financial Inclusion (2019). Digital Financial Inclusion in Peru; A Promising Trend to Watch. Retrieved from: <https://www.centerforfinancialinclusion.org/digital-financial-inclusion-in-peru-a-promising-trend-to-watch>.

Chirchir, R., Barca, V. (2020). Building an integrated and digital social protection information system. Retrieved from: <https://socialprotection.org/sites/default/files/publications_files/GIZ_DFID_IIMS%20in%20social%20protection_long_02-2020.pdf>.

The Bureau of National Affairs. (2015). Privacy in Latin America and the Caribbean. Retrieved from: <https://www.bna.com/uploadedFiles/BNA_V2/Legal/Pages/Custom_Trials/PVRC/Privacy_Laws_Latin_America.pdf>.

Campello, T., Neri, M. C. (2014). Bolsa Família Program: a decade of social inclusion in Brazil. Brasília. Ipea.

Carmona, S. C. (2019). Biometric technology and beneficiary rights in social protection programmes. International Social Security Review. 4 (72), 3-28.

Caruso, C. (2016). Digital Financial Inclusion in Peru; A Promising Trend to Watch. Retrieved 30 March, from: <https://www.centerforfinancialinclusion.org/digital-financial-inclusion-in-peru-a-promising-trend-to-watch>.

Center for Global Development. (2017a). Identification Revolution: Can Digital ID Be Harnessed for Development?. Retrieved from: <https://www.

cgdev.org/sites/default/files/identification-revolution-can-digital-id-be-harnessed-development-brief.pdf>.

Center for Global Development (2017b). Identification as a National Priority: The Unique Case of Peru. Retrieved from: <https://www.cgdev.org/sites/default/files/identification-national-priority-unique-case-peru.pdf>.

Center of Excellence for CRVS Systems. (2020). Gender equality. Retrieved 30 March, from: <https://crvssystems.ca/gender-equality>.

Clavijo, S., Vera, N., Londoño, J., Beltrán, D. (2019). Digital Financial Services (FINTECH) in Latin America. Retrieved from: <https://www.anif.com.co/sites/default/files/investigaciones/anif-fintech-wpaper0219.pdf>.

Chrispino, R. (2019, September). Identidade como acesso à cidadania. (COSTA. J, Interviewer).

Comisión Multisectorial de Inclusión Financiera. (2015). Estrategia Nacional de Inclusión Financiera. Retrieved from: <http://www.mef.gob.pe/contenidos/archivos-descarga/ENIF.pdf>.

Comisión Nacional de Arbitraje Médico. (2018). El expediente clínico electrónico universal en México. Mexico. Retrieved from <http://www.conamed.gob.mx/gobmx/boletin/pdf/boletin18/expediente.pdf>.

Cortés, R. A. (2019). El nuevo entorno regulatorio de la protección de datos personales en Chile. Retrieved 30 March, from: <https://iapp.org/news/a/el-nuevo-entorno-regulatorio-de-la-proteccion-de-datos-personales-en-chile/>.

Dreze, J., Khalid, N., Khera, R., Somanchi, A. (2017). Pain without gain? Aadhaar and food security in Jharkhand.Economic and political weekly. Vol. 52, Issue No. 50. Retrieved 30 March, from: <https://www.epw.in/journal/2017/50/special-articles/aadhaar-and-food-security-jharkhand.html>.

Domínguez, M. (2018). Access and use of information and communication technologies in Mexico: determining factors. PAAKAT: Revista De Tecnología Y Sociedad. Vol. 8 No. 14. Retrieved 30 March, from <http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-36072018000200002&lang=pt>.

ECLAC (2015). Inclusive social development: The next generation of policies for overcoming poverty and reducing inequality in Latin America and the Caribbean. Santiago de Chile. Retrieved from: <https://repositorio.cepal.org/bitstream/handle/11362/39101/4/S1600098_en.pdf>.

Enríquez, O. (2018). Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento. Revista IUS, 12(41), 267-291. Retrieved 10 December 2019, from <http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472018000100267&lng=es&tlng=es>.

Escócia, F. (2019a). Invisíveis: uma etnografia sobre identidade, direitos e cidadania nas trajetórias de brasileiros sem documento. Retrieved from: <http://www.mprj.mp.br/documents/20184/151138/escossiafernandameloda.invisiveis_umaetnografiasobreidentida.pdf>.

Escóssia, F. (2019b, September). Identidade como acesso à cidadania. (COSTA. J, Interviewer). Retrieved 30 March, from: <https://www.youtube.com/watch?v=8yK3FHEnpnA>.

FAFT. (2014). Guidance for a Risk-Based Approach The Banking Sector. Retrieved from: <https://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf>.

FATF. (2019). Public consultation on FATF draft guidance on digital identity. Retrieved 30 March, from: <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/consultation-digital-id-guidance.html>.

Ferrari, M. G. Marcas de identidad. Juan Vucetich y el surgimiento transnacional de la dactiloscopia (1888-1913). Rosario: Prohistoria Ediciones, 2015.

Gelb, A., Metz, A. D. (2018). Identification Revolution: Can Digital ID Be Harnessed for Development? Center for Global Development. Washington, DC.

Gelb, A., Mukherjee, A., Navis, K., Thaplyal, M., Giri, A. (2017). What a New Survey of Aadhaar Users Can Tell Us About Digital Reforms: Initial Insights from Rajasthan. Center for Global Development. CGD Notes. Retrieved 30 March, form: <www.cgdev.org/publication/what-a-new-survey-aadhaar-users-can-tell-us-about-digital-reforms-initial-insight>.

Gelb, A., Mukherjee, A., Navis, K., (2020). How Can Digital ID and Payments Improve State Capacity and Effectiveness? Center for Global Development Notes. Retrieved from <https://www.cgdev.org/sites/default/files/citizens-and-states-how-can-digital-id-and-payments-improve-state-capacity.pdf>.

Gobierno Digital Chile. (2019). División de Gobierno Digital. Retrieved 30 March, from <https://digital.gob.cl/plan/identidad-digital>.

Gobierno Digital Chile. (2018). Estrategia de Transformación Digital del Estado: Estado al Servicio de las Personas. Retrieved from: <https://digital.gob.cl/doc/estrategia_de_transformacion_digital_2019_.pdf>.

GSMA. (2016.) Digital identity as a key enabler for e-government services. Retrieved from: <https://www.gsma.com/identity/wp-content/uploads/2016/02/MWCB16-Digital-Identity-as-a-Key-Enabler-for-eGovernment-Services-Marta-Ienco.pdf>.

GSMA. (2016). Digital Identity: a prerequisite for Financial Inclusion?. Retrieved 30 March, from: <https://www.gsma.com/mobilefordevelopment/country/global/digital-identity-a-prerequisite-for-financial-inclusion/>.

Hellmann, A. G. (2015). How does Bolsa Familia work?: Best practices in the implementation of conditional cash transfer programs in Latin America and the Caribbean. IADB. Retrieved 30 March, from: <https://publications.iadb.org/en/how-does-bolsa-familia-work-best-practices-implementation-conditional-cash-transfer-programs-latin>.

Hunter, W., Brill, R. (2016). “Documents, Please”: Advances in Social Protection and Birth Certification in the Developing World. World Politics, 68(2), 191-228. doi:10.1017/S0043887115000465

Hunter, W. (2019). Identity Documents, Welfare Enhancement, and Group Empowerment in the Global South. The Journal of Development Studies, 55(3), 366-383, doi: 10.1080/00220388.2018.1451637

IADB. (2017). La gestión de la identidad y su impacto en la economía digital. Retrieved from: <https://www.alejandrobarros.com/wp-content/uploads/2016/04/Gestion-de-la-identidad-y-su-impacto-en-la-economia-digital.pdf>.

IADB. (2019). Registros civiles y oficinas de identificación: Análisis y fichas de país. Retrieved from: <https://publications.iadb.org/publications/spanish/document/Registros_civiles_y_oficinas_de_identificaci%C3%B3n_an%C3%A1lisis_y_fichas_de_pa%C3%ADs_es.pdf>.

Ibarra, A. B., Byanyima, W. (2016). Latin America is the world’s most unequal region. Here’s how to fix it. Retrieved 30 March, from: <https://www.weforum.org/agenda/2016/01/inequality-is-getting-worse-in-latin-america-here-s-how-to-fix-it/>.

ITU News. (2019). Unique, legal and digital: Three characteristics of ID crucial to financial inclusion. Retrieved 30 March, from: <https://news.itu.int/unique-legal-digital-id-financial-inclusion/>.

Laval, C. E. P. (2018). Utopías de control detrás de la identificación civil: los proyectos de identificación de Clodomiro Cabezas Cabezas. Chile, 1927-1938, Revista Historia y Justicia. Retrieved 30 March, from: <https://doi.org/10.4000/rhj.1260>.

Lindert, K., Linder, A., Hobbs, J., Briere, B. (2007). The Nuts and Bolts of Brazil's Bolsa Família Program: Implementing Conditional Cash Transfers in a Decentralized Context. World Bank Group. Retrieved from: <http://documents.worldbank.org/curated/pt/972261468231296002/pdf/398530SP1709.pdf>.

Loufield, E., Vashisht, S. (2020). Data Consent: Let's Share the Burden for Effective Consumer Protection. Center for Financial Inclusion. Retrieved 30 May from: <https://www.centerforfinancial-inclusion.org/data-consent-lets-share-the-burden-for-effective-consumer-protection>.

Masiero, S. (2017). Digital governance and the reconstruction of the Indian anti-poverty system. Oxford Development Studies, 45 (4), 393-408.

Masiero, S. (2019). The Digitalization of Anti-poverty Programs: Aadhaar and the Reform of Social Protection in India. Digital Economies at Global Margins. Ed. Mark Graham. MIT Press Direct.

Mastercard. (2019a). Digital Identity: Restoring Trust in a Digital World. Retrieved from: <https://www.mastercard.us/content/dam/mccom/en-us/issuers/digital-identity/digital-identity-restoring-trust-in-a-digital-world-final-share-corrected.pdf>.

Mastercard. (2019b). Examining the Latin American and Caribbean E-commerce Market. Retrieved from: <https://newsroom.mastercard.com/latin-america/files/2019/12/Whitepaper-Digital-Security-mastercard-ENG-simples-FINAL2.pdf>.

McKinsey Global Institute (2019). Digital identification: A key to inclusive growth. Retrieved 30 March, from: <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth>.

Mexico Digital. (2018). Certificado Electrónico de Nacimiento. Retrieved 13 December 2019, from: <https://www.gob.mx/mexicodigital/articulos/certificado-electronico-de-nacimiento-142911>.

Mexico Digital. (2014). Certificado Electrónico de Nacimiento. Retrieved 13 December 2019, from: <https://www.gob.mx/mexicodigital/articulos/certificado-electronico-de-nacimiento>.

Ministry of Social Development Brazil. (2015). Guia de Cadastramento de Famílias Indígenas. MDS. Brasília.

Muralidharan, K., Niehaus, P., Sukhtankar, S (2020). Identity Verification Standards in Welfare Programs: Experimental Evidence from India. National Bureau of Economic Research Working Paper, 26744

Muralidharan, K., Niehaus, P. & Sukhtankar, S. (2016). Building state capacity: Evidence from biometric smartcards in India. American Economic Review 106 (10), 2895-2929.

Murthy, G. & Medine, D. (2018). Data Protection and Financial Inclusion: Why Consent Is Not Enough. Blog Series: Data Privacy and Protection. Consultative Group to Assist the Poor. Retrieved 30 March, from: <http://cgap.org/blog/data-protection-and-financial-inclusion-why-consent-not-enough>.

Muzzi, M. (2010). Good Practices in Integrating Birth Registration into Health Systems

(2000-2009). Unicef. Retrieved from: <https://www.unescap.org/sites/default/files/UNICEF-birth-registration-in-health-systems.pdf>.

OEA. (2008). Diagnóstico del marco jurídico-institucional y administrativo de los sistemas de Registro Civil en América Latina. PUICA. Retrieved from: <http://www.oas.org/sap/docs/puica/diagnostico_legal_administrativo.pdf>.

OECD. (2001). Understanding the Digital Divide. OECD Digital Economy Papers, No. 49, OECD Publishing, Paris, page 5. Retrieved 30 March, from: <https://doi.org/10.1787/236405667766>.

OECD. (2009). The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers. OECD Digital Economy Papers. (Report No. 160). OECD Publishing, Paris. Retrieved 30 March, from <https://doi.org/10.1787/20716826>.

OECD. (2019a). Shaping the Digital Transformation in Latin America: Strengthening Productivity, Improving Lives, OECD Publishing, Paris. Retrieved 30 March, from: <https://doi.org/10.1787/8bb3c9f1-en>.

OECD. (2019b). Harnessing the Digital Transformation to Boost Productivity in Latin America and the Caribbean. Retrieved 30 March, from: <https://www.oecd.org/about/secretary-general/harnessing-digital-transformation-to-boost-productivity-in-lac-colombia-october-2019.htm>.

OECD. (2019c). Digital Government in Chile – Digital Identity. Retrieved from: <https://www.oecd-ilibrary.org/sites/9ecba35e-en/index.html?itemId=/content/publication/9ecba35e-en&mimeType=text/html>.

OECD (2019d). Strengthening Digital Government. Retrieved from: <https://www.oecd.org/going-digital/strengthening-digital-government.pdf>.

OECD (2019e). Digital Government in Chile – A Strategy to Enable Digital Transformation, OECD Digital Government Studies, OECD Publishing, Paris. Retrieved from: <https://doi.org/10.1787/f77157e4-en>.

Pan American Health Organization (PAHO). (2016). eHealth in the Region of the Americas: breaking down the barriers to implementation. Retrieved 30 March, from: <https://iris.paho.org/bitstream/handle/10665.2/31286/9789275119259-eng.pdf?sequence=6&isAllowed=y>.

Peirano, M. (2009). O paradoxo dos documentos de identidade: relato de uma experiência nos Estados Unidos. Retrieved from: <http://www.mprj.mp.br/documents/20184/151138/peirano,mariza.oparadoxodosdocumentosdeidentidade.pdf>.

Privacy International. (2012). Medical privacy and security in developing countries and emergency situations. Retrieved from: <https://privacyinternational.org/sites/default/files/2018-11/Privacy_International_Medical_Privacy.pdf>.

Privacy International. (2018). Liliana: "If you don't have RUT, you can't do it.". Retrieved 30 March, from: <https://privacyinternational.org/case-study/2545/liliana-if-you-dont-have-rut-you-cant-do-it>.

Ramada-Sarasola, M. (2012). Can Mobile Money Systems Have a Measurable Impact on Local Development?. Retrieved 30 May from: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2061526>.

Ratcliffe, R. (2019). How a glitch in India's biometric welfare system can be lethal. Automating poverty Series. The Guardian. Retrieved 30 March, from <https://www.theguardian.com/technology/2019/oct/16/glitch-india-biometric-welfare-system-starvation>.

Ramanathan, U. (2014). Biometrics Use for Social

Protection Programmes in India Risk Violating Human Rights of the Poor. Retrieved 30 March, from: <http://www.unrisd.org/sp-hr-ramanathan>.

Sepúlveda, M. (2019). Data Protection is Social Protection. Retrieved 30 May from: <https://www.project-syndicate.org/commentary/social-protection-biometric-data-privacy-by-magdalena-sep-lveda-2019-04?barrier=accesspaylog>.

Tase TH, Lourenção DCA, Bianchini SM, Tronchin DMR (2013). Patient identification in healthcare organizations: an emerging debate. Rev Gaúcha Enferm.;34(2):196-200.

UN. (2018). E-Government Survey: Gearing e-government to support transformation towards sustainable and resilient societies. Retrieved from: <https://publicadministration.un.org/Portals/1/Images/E-Government%20Survey%202018_FINAL%20for%20web.pdf>.

UN Secretary-General. (2019). Secretary-General's opening remarks to the High-level Event on "10 Years of Financial Inclusion - Vast Progress and Challenges Ahead". Retrieved 30 March, from: <https://www.un.org/sg/en/content/sg/statement/2019-09-25/secretary-generals-opening-remarks-the-high-level-event-10-years-of-financial-inclusion-vast-progress-and-challenges-ahead-delivered>.

UNAIDS. (2014). Considerations and guidance for countries adopting national health identifiers., Geneva, 17 April 2014. Retrieved from: <https://www.unaids.org/sites/default/files/media_asset/JC2640_nationalhealthidentifiers_en.pdf>.

UNCDF. (2020). Financial Inclusion and the SDGs. Retrieved 30 May from: <https://www.uncdf.org/financial-inclusion-and-the-sdgs>.

UNESCO and the Regional Bureau for Sciences in Latin America and the Caribbean (2017). Sociedad digital: brechas y retos para la inclusión digital en América Latina y el Caribe. Retrieved 30 March, from: <https://unesdoc.unesco.org/ark:/48223/pf0000262860>.

UNESCO. (2009). Regional overview: Latin America and the Caribbean. Retrieved from: <https://en.unesco.org/gem-report/sites/gem-report/files/178428e.pdf>.

UNICEF. (2018). Latin America and the Caribbean: a decade lost in ending child marriage. Retrieved 30 May from: <https://www.unicef.org/press-releases/latin-america-and-caribbean-decade-lost-ending-child-marriage>.

UNRISD. (2010). Combating Poverty and Inequality: Structural Change, Social Policy and Politics. Retrieved from: <http://www.unrisd.org/80256B3C005BCCF9/(httpAuxPages)/92B1D5057F43149CC125779600434441/$file/PovRep%20(small).pdf>.

UNU-WIDER. (2016). Cash transfers in Latin America: Effects on poverty and redistribution. Retrieved 30 May from: <https://www.wider.unu.edu/publication/cash-transfers-latin-america>.

Villarreal, F. G. (ed.). (2017). Inclusión financiera de pequeños productores rurales, Libros de la CEPAL, N° 147 (LC/PUB.2017/15-P), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2017. Retrieved 30 March, from: <https://repositorio.cepal.org/bitstream/handle/11362/42123/S1700277_es.pdf?sequence=1&isAllowed=y>.

Vucetich, J (1916). Comment in the Creation of the Identity Law of (Ley de Registro de Identidad de las Personas). Registro General de Identificación. Argentina.

Whitley, E. A. (2018). Trusted Digital Identity Provision: GOV.UK Verify's Federated Approach. CGD Policy Paper. Washington, DC: Center for Global Development. Retrieved 30 March, from: <https://

www.cgdev.org/publication/trusted-digital-identity-provision-gov-uk-verify-federated-approach>.

World Bank (2016). Identification Principles for Sustainable Development: toward the digital age. Retrieved from World Bank ID4D website <http://documents.worldbank.org/curated/en/213581486378184357/pdf/112614-REVISED-English-ID4D-IdentificationPrinciples-Folder-web-English-ID4D-IdentificationPrinciples.pdf>.

World Bank. (2018a). G20 Digital Identity Onboarding. Retrieved from: <https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf>.

World Bank. (2018b). Global ID Coverage, Barriers, and Use by the Numbers: Insights from the ID4D-Findex Survey. Retrieved from: <http://documents.worldbank.org/curated/en/953621531854471275/Global-ID-Coverage-Barriers-and-Use-by-the-Numbers-Insights-from-the-ID4D-Findex-Survey.pdf>.

World Bank (2018c). The Role of Digital Identification for Healthcare: The Emerging Use Cases. Washington, DC: World Bank License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO); Retrieved from World Bank ID4D website <http://documents.worldbank.org/curated/en/595741519657604541/The-Role-of-Digital-Identification-for-Healthcare-The-Emerging-Use-Cases.pdf>.

World Bank. (2018d). Guidelines for ID4D Diagnostics. Retrieved from: <http://documents.worldbank.org/curated/en/370121518449921710/Guidelines-for-ID4D-Diagnostics.pdf>.

World Bank (2019a). Inclusive and Trusted Digital ID Can Unlock Opportunities for the World’s Most Vulnerable. Retrieved 13 December, from: <https://www.worldbank.org/en/news/immersive-story/2019/08/14/inclusive-and-trusted-digital-id-can-unlock-opportunities-for-the-worlds-most-vulnerable>.

World Bank (2019b). ID4D Practitioner’ Guide, Version 1.0 (October 2019). Washington, DC. Retrieved from: <http://documents.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf>.

WHO. (2007). Patient Identification. Retrieved from: <https://www.who.int/patientsafety/solutions/patientsafety/PS-Solution2.pdf>.

WHO & ITU. (2012). National eHealth Strategy Toolkit. Retrieved from: <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-E_HEALTH.05-2012-PDF-E.pdf>.

World Economic Forum (2018). The appropriate use of Customer Data. Retrieved from: <http://www3.weforum.org/docs/WP_Roadmap_Appropriate_Use_Customer_Data.pdf>.

World Economic Forum. (2020). Passwordless Authentication: The next breakthrough in secure digital transformation. Retrieved 30 March, from: <https://www.weforum.org/whitepapers/passwordless-authentication-the-next-breakthrough-in-secure-digital-transformation>.

ITS

Funded by

ON

OMIDYAR NETWORK

Find us online

itsrio.org