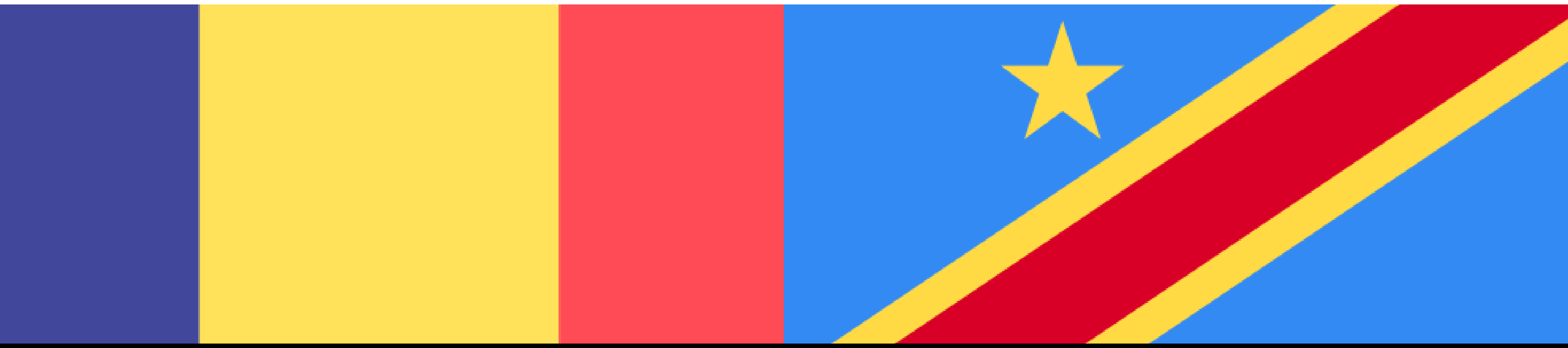
Policy Brief

Internet freedoms in Chad and DRC:

Better understanding the notion of digital identity



Policy Brief

Internet freedoms in Chad and DRC: Better understanding the notion of digital identity

March 2022.

By **Rigobert Kenmogne,** Programs Officer, Paradigm Initiative.

Design and Layout by
Kenneth Oyeniyi, Communications Assistant, Paradigm Initiative.

Published By
Paradigm Initiative

Supported by
DRL

PARADIGM
INITIATIVE

@ParadigmHQ

1.0 Executive summary

Respect for a person's digital identity is guaranteed in almost all countries in the world, including the Democratic Republic of Congo and the Republic of Chad. The local, regional and international legal texts that ensure the protection of this domain are generally violated or misinterpreted by policy makers, technological structures and certain private users.

This policy brief aims to present the situation of digital identity as an essential part of personal data, to better present the various types of digital identity, the forms of violation of identities and interactions on privacy that can be committed on digital networks and related protection mechanisms.

The difference between digital identity and civil identity is highlighted so as to clearly distinguish the two. The five types of digital identity are often the subject of numerous attacks. This is the case with electronic searches, unauthorized copies of data, duplication of digital identity, control and monitoring of people based on their digital identity by agents of state and private services.

Due to violations of digital identities on the Internet and in social networks, this requires a new management system with an extensive legal environment and credible actors.

A certain number of legal mechanisms nevertheless make it possible to combat or curb violations of digital identities. Compliance with these legal instruments requires compliance with the key principles that guide digital identity in the Internet ecosystem.

2.0 Introduction

Digital rights are the collection of human rights online in the internet age. The presence of users online has always been a subject of reflection on the interaction between the latter and the machines that interconnect them.This way of interacting in the digital ecosystem raises questions about identity on the Internet. The users on the internet are represented, grouped together and interact with each other while respecting the standards that are established or that evolve is critical. This question on digital identity comes after several months of social networks shutdown in Chad by the government.[1] In this phase of censorship of social media, some Chadians, internet users have also mentioned a violation of their digital identity by the government .[2] A better understanding and knowledge of the contours of the notion of digital identity in a context of recurrent violations of digital rights is necessary. The DRC government has also repeatedly censored social media, some sites and online users[3]. The question on the understanding of the concept for the users in the two countries remains relevant.

[1] Chad, the country where social networks have been blocked for a year, BBC.com(2019) https://www.bbc.com/afrique/region-47737334 (accessed 26 January 2022).

[2] Digital security in Chad, Ritimo.org(2021) https://www.ritimo.org/Fiche-pays-securite-numerique-Tchad (accessed January 26 2022).

[3] Ibidem

Digital identity[4] is defined as a technological link between a real entity and virtual entities. It allows the identification of the individual online as well as the connection of this one with all the virtual communities present on the Web. Digital identities are information such as login and password, but also all traces and activities associated with the activities and the user.

Data breaches related to personal data on the Internet in the DRC show that the country's Internet ecosystem does not have a clear mastery of digital identity and interactions with digital rights. Violations of digital rights in the country in recent years, including online surveillance or controlThe mismanagement of digital identities encourages violations of digital rights, in particular the surveillance or control of online users. These actions outside the legal framework are violations. This is happening in a context of legal vacuum since the DRC does not have a law on personal data protection.

In Chad, the government and technological services use digital identities to censor the Internet on certain private networks or to control political adversaries. Digital identity management falls under the first component of digital law on the management of private or personal data.

There are a large number of international legal instruments that protect digital identity through privacy principles. The Universal Declaration of Human Rights adopted and proclaimed by the General Assembly of the United Nations in its resolution 217 A (III) of December 10, 1948.[5] Alongside this, it is worth mentioning several international treaties ratified by the Democratic Republic of Congo and Chad. This is the case of the International Covenant on Economic, Social and Cultural Rights,[6] the International Covenant on Civil and Political Rights[7]; the Convention relating to the Status of Refugees;[8] of the African Charter on Human and Peoples' Rights[9]. The two constitutions of DR Congo and Chad. The Congolese constitution in article 2 maintains that "in the Democratic Republic of Congo, the exercise of individual and collective rights and freedoms is guaranteed subject to respect for the law, public order and good morals"[10]. The "Constitutional Act of the Transition" of DRC defines and protects fundamental human rights. Article 13(1) provides that "the freedom of the human person is inviolable".

Between 2018 and 2021, several types of digital rights violations were recorded in the DRC and Chad. Some attacks on digital identity are legitimized by state security. This is because digital identities are not well known to digital users and some violations pass

[4] Digital identity(2020) https://www.digitalidentity.gov.au/ (accessed 10 January 2022).

[5] Article 12 de cette Déclaration dispose : "Nul ne sera l'objet d'immixtion arbitraire dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes"(accessed 10 january 2022).

[6] UN International Covenant on Civil and Political Rights https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx (1976)(accessed 10 January 2022).

[7] Office of the United Nations High Commissioner for Human Rights (1976) https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx (accessed 10 January 2022).

[8] The 1951 Refugee Convention and 1967 Protocol(1967) https://www.unhcr.org/1951-refugee-convention.html (accessed 11 January 2022).

[9] African Charter on Human and Peoples' Rights) https://www.achpr.org/legalinstruments/detail?id=49 (accessed 11 January 2022).

[10] Décret-loi constitutionnel n°003 du 27 mai 1997 relatif à l'organisation et à l'exercice du pouvoir en République Démocratique du Congo.

before their eyes.

The legal level of identity has no real definition, the doctrine indicates that identity is the set of elements in which it is established that a person is indeed the one who is said or presumed to be such through the last name, first name, last name, nationality, parentage. It must make it possible to legally impute acts and facts to a given person. , specify Maryline Laurent and Samia Bouzefrane. He has to specify that the arrival of the virtual world multiplies the modes of identification. Identity in the digital age has blurred contours. It cannot be defined by an entity freely composed by the person himself. In its social dimension, identity is built around online self-representation, through blogs, social networks, and the dissemination of functioning communication tools dedicated to self-representation.[11]

Today, the concept of Internet identity and digital rights is much richer and broader with the rise of social media platforms that have billions of users, including Facebook, YouTube, WhatsApp, Messenger, Twitter and others.

3.0 Digital identities and civil identity

The digital identity should not be confused with the civil identity of the person who gives it legal personality, acquired by the establishment of a birth certificate and extinguished by a death certificate drawn up by a civil servant. The civil identity of a person is signified by his name, his first name, his address etc. Digital identity, on the other hand, includes a username, password and email address, etc. These usernames are associated with accounts which themselves contain hundreds of thousands of data, often of a personal nature. The death of a person does not result in the erasure of their digital identity, among others on social networks, unless the conditions of service indicate it.[12] There are privacy considerations and specific use cases for each type of digital identity.

4.0 Types of digital identities on the Internet

There are five types of identities on the Internet. Users on the platforms can be identified by one or all types of identities at a time depending on the platforms in which they interact.

1. Electronic identities. Some governments issue electronic identities to their citizens for online use. In some cases, the issued identity, or the identity provider, is an approved body (eg Ministry of Post). To receive an electronic identity from the government, citizens typically need to confirm their identity by presenting a government-issued passport, ID card, or other form of government-issued identification. Therefore, the two types of identity are linked. In general, government-issued electronic identities are primarily used by government services; for example, tax returns or a claim for benefits. Secondary uses are usually for services requiring a high degree of certainty or the assurance that the person is who he or she claims to be (for example, banking and medical records). Government-issued electronic identities mostly have multiple functions, such as identification,

[11] Gestion des identités numériques, Contrepoint (2019) https://www.contrepoints.org/2019/09/11/353261-la-gestion-des-identites-numeriques (accessed 15 January 2022).
[12] « Respecter la vie privée et le droit à l'image - Internet responsable »(2019) www.eduscol.education.fr   (consulté le 12 Janvier 2022).

two-factor authentication to access online services (e.g. virtual government services). They can be used as electronic information proving the possession of a passport to access personal data, and as a legally valid electronic signature.

2. Identities based on an attribute. Some interactions do not require identification. Instead, the person only needs to have a specific attribute (for example: be at least 18 years old or be a student).

3. Indeed, while an attribute (e.g. age) might not indicate the actual identity of an individual, a combination of attributes may make this possible (e.g. date of birth, postal code or sex).

4. Identities based on authentication. Many online service providers, such as Facebook and Gmail, allow users to access their account through a username and password. These identities represent how customers identify with service providers and how service providers authenticate or verify that users are who they claim to be. Unlike government-issued electronic identities, login credentials can be anonymous or pseudonyms. Second generation authentication mechanisms, such as "single sign-on", allow users to connect to multiple services from one access point. For various reasons, authentication mechanisms requiring only a username and password are certainly not secure. Today, many service providers offer additional access control protection through two-factor authentication. This type of authentication requires a combination of something the user receives (for example, an expiring one-time code sent to the user's smartphone) and something that the user knows (for example, the name of user or password).

5. Electronic signatures. Many countries have adopted laws to recognize the legal status of electronic signatures. In addition to being a means of identification, electronic signatures can have repercussions such as the confirmation or acceptance of a contract online. Electronic signatures often have two functions: confirming that the user assumes the content of a document and confirming the author of the message. Cross-border legal recognition of electronic signatures is essential for efficient international trade.

6. Identifiers. Identifiers are data that identifies information about a device and / or user. Device information may include device type, operating system, browser version, browser, plugins, etc. Device information may include preferences, such as font size, screen colors, and contrast, and similar characteristics. All online interactions involve the use of identifiers. Some perform the function of the Internet (e.g. IP addresses), others identify or recognize a device and / or user (e.g. security in financial institutions), and still others track interactions online users (targeted advertising on Facebook for example). The internet area has several identifiers. Identifiers can be used to identify a specific device or user or to track a device or the device user's online interactions. Some identifiers can be noticed easily (e.g. browser functionality), others are deliberately placed in a device for easy tracking (e.g. cookies). Identifiers can be grouped, linked, and used to determine connections.

5.0 Managing digital identities on the Internet

Integrity, risk, security, trust and confidentiality are major issues specific to digital identity on the Internet. However, the level of involvement of the user in the management of his digital identity differs according to the importance of the subject and his level of interaction. However, it is essential for an individual to manage his digital identity, the risk being that if the digital identity is not managed directly by the individual, he leaves it to others to create it and he is thus exposed to certain abuses such as a bad reputation, the hacking of certain information[13], or quite simply being faced with undesirable situations.

According to Maryline Laurent,[14] professor of computer networks at Télécom Sud Paris and Samia Bouzefrane,[15] lecturer in information at the CNAM in Paris, identity management is done in two main ways.

First, it can be done by the federation of identities that allows a set of applications to refer to a single user, while the same user is known under different identities of each application. On combines identity to the federation of thematic the mechanisms to propagate identity from one application to another on the Internet. Butfor almost 20 years, with the emergence of the concept of Cloud computing, identity management has undergone a profound transformation and is enjoying ever-increasing success towards an inescapable reality of the evolution of the Internet. According to these two researchers, despite the enormous possibilities offered by Cloud computing in terms of pooling services and savings, it also entails numerous risks relating in particular to the security of user data.

6.0 Digital Identity on social media

Platforms and social networks have diversified the concept of digital identity. The network Facebook, for example, asks users to use “the name you use every day”23. It is a policy less rigid than the civil status which makes it possible to adapt better to particular cases. Those in charge of the platform find in this desire the source in the DNA of the social network: a network for students at the base where everyone had to decline their identity. According to the former marketing director of Facebook, Randi Zuckerberg, “the use of real names is also explained by the fact that” Internet users remain more measured in what they say when their real identity is at stake and be more constructive[16]:

This desire is also recalled in the conditions of use of the social network and “Facebook’s requirement for the use of a real name creates a more secure environment. (...) When people voice their opinions and act using their true identity and reputation, our community becomes more responsible.”[17]

Facebook maintained its position in the use of the real name of the user on the platform. Alex Schultz says that “when people use the name that other people know they are more responsible for what they say, which makes it harder to hide behind an anonymous name to harass, intimidate, spam or scam someone”.

[13] Qu’est-ce que le hacking ?(2021) https://www.avast.com/fr-fr/c-hacker (accessed 18 January 2022).
[14] Maryline Laurent (2020) http://www-public.imtbs-tsp.eu/~lauren_m/ (accessed 12 Janvier 2022).
[15] https://samia.roc.cnam.fr/
[16] Facebook: “Anonymity on the Internet has to go away”(2011) https://www.zdnet.com/article/facebook-anonymity-on-the-internet-has-to-go-away/ (accessed 15 January 2022).
[17] Ibidem

7.0 Types of digital Identity Breaches

In the United States, a digital identity theft law called: Identity theft penalty enhancement act exists to increase the jail time for digital identity thieves who commit an offense. It was adopted on June 16, 2005. Since the beginning of 2011 in California, a law has been promulgated by the Governor of California to once again punish identity theft.

In the DRC and Chad, no law yet exists on the mismanagement of digital identities. The violations recorded in these two countries on digital identity and personal data are in opposition to principle 40(1) on privacy and the protection of personal information of the African Commission on Human and Peoples' Rights Declaration of Principles on Freedom of Expression and Access to Information which states that "everyone has the right to privacy, including the confidentiality of their communications and the protection of their personal information." [18]

8.0 Guiding Principles on Internet Identity

To ensure better management of digital identities, governments in DRC and CAR and data management companies must take into account a number of guiding principles. Individuals should have the option of using digital identities such as pseudonyms or anonymous, depending on the context in which they interact with other people. Also, individuals should have access to reliable, secure digital identities, taking into account respect for privacy from the design of online transactions and particularly those containing sensitive data such as medical data (eg: data on COVID-19-19) and financial or any private content. Basically, these are the characteristics that promote a secure, reliable and protective online expression environment with low possibility of digital rights infringement.

Digital identities do not have to be government-issued to be trusted. However, governments should consider offering electronic identification for more secure access to virtual government services and business transactions (eg: banking transactions, diplomatic information) that require a high level of authentication.

Governments in DRC and CAR, that have already issued electronic identification (identity providers) should take into account the following principles for the security of online users and avoid any violations:

1. Examine all forms of electronic identity most appropriate for the intended uses; and identify economic, social, cultural or other obstacles that could prevent their deployment or use.
2. Ensure that their electronic identity system is technically interoperable and legally compatible with identity systems deployed by other governments, so that their electronic identities can be used in international transactions.
3. Prevent government and other parties that use it from tracking electronic identity use between departments and institutions, unless absolutely necessary and urgent. It is good privacy and security practice to quarantine the use of digital identities and the data used to access them.

[18] African Commission on Human and Peoples' Rights Declaration of Principles on Freedom of Expression and Access to Information (2019). See principle 40 https://www.achpr.org/public/Document/file/English/Declaration%20of%20Principles%20on%20Freedom%20of%20Expression_ENG_2019.pdf (accessed 5 december 2021).

4. Collect and use only the data necessary during the entire electronic identity life cycle.
5. Applying the principle of data minimization in this way increases consumer confidence as well as choice.
6. Make electronic identities revocable when needed (for example, in the event of compromise or theft).
7. Carry out an in-depth analysis of the risks and benefits before considering using biometric data for electronic identity purposes. In the event of a compromise, the biometric data is irrevocable (for example, you cannot change your fingerprint). For this reason, this should be avoided, unless it is absolutely necessary.
8. Governments should ensure that citizens to whom they have not issued electronic identities are not excluded from government services.

9.0 Conclusion

An effective digital identity promotes secure exchanges on the Internet. For this reason, it is essential that governments in the both countries continue to encourage the open development and use of new technologies to express one's identity on the Internet, whether identified, pseudonymous, or anonymous; and refrain from any activity that may hinder innovation or economic and social progress, such as requiring a level of identification required to access the Internet or social media.

The analysis of the contours of digital identity and the interactions between privacy and personal data help to restore and limit violations of digital identities for natural or legal persons online.

In the context of regular privacy breaches in Chad and in DRC, the digital identities of certain opponents, activists or influencers have often been abused for reasons of surveillance or control. Digital rights violations in these countries can permanently challenge digital identities (electronic identities issued by governments) and make the Internet ecosystem in these countries unreliable and secure.

10.0 Recommendations

These recommendations help the better management of digital identities in Chad and DRC.

1. The DRC must facilitate the establishment of a law on personal data and on the protection of digital identities. Chad has a law on the protection of personal data, but it is not sufficiently applied. Chad must strengthen the protection of digital identities based on current legal provisions.
2. To limit violations, the two countries must define a digital identity protection charter.
3. To strengthen the management of digital identities, governments can set up a digital identity management agency in the DRC with regard to the size of the population.
4. Governments must commit to limiting political interactions in the management of digital identities.
5. Governments must public online platforms define their commitment to the protection of digital identities in specifications.
6. For a better sharing of experience, public authorities and organizations of society must be trained for better management of digital identities and techniques for protection against violations.

11.0 Additional resources

The boss of Twitter victim of identity theft on his own social network https://www.lesechos.fr/tech-medias/hightech/le-patron-de-twitter-victime-dusurpation-didentite-sur- his-own-social-network-1128042

Understanding Your Identity Online: Identity Overview, 2011, http://www.internetsociety.org/understanding-your-online-identity-overview-identity

Understanding Your Identity Online: Protecting Your Privacy, 2012, http://www.internetsociety.org/understanding-your-online-identity-protecting-your-privacy-0

R. Wilton, Have you chosen an identity provider recently ?, 2014, http://www.internetsociety.org/doc/have-you-chosen-identity-provider-lately

More information about online digital identity can be found online.

Digital Identity Management: Fostering Innovation and Confidence in the Internet Economy, Organization for Economic Co-operation and Development, 2011, http://www.oecd.org/sti/interneteconomy/49338380.pdf

E. Birrell and FB Schneider, "Federated Identity Management Systems: A Privacy-Based Characterization," Security & Privacy, IEEE, vol. 11, no. 5, September-October 2013, pp. 36–48, https://www.cs.cornell.edu/fbs/publications/idMgmt.SP.pdf