

Ranking Digital Rights in Angola, Democratic Republic of Congo and Central African Republic

An analysis of Unitel-Angola, Orange-DRC and Orange CAR





December 2021

Authors:

Bulanda T Nkhowani, Rigobert Kenmogne

Editorial Team:

Thobekile Matimbe, Nnenna Paul-Ugochukwu

Design and Layout:

Kenneth Oyeniya



Creative Commons
Attribution 4.0 International (CC BY 4.0)



PARADIGM
INITIATIVE



@ParadigmHQ

01



Introduction

Ranking Digital Rights (RDR) works to promote freedom of expression and privacy on the Internet by creating global standards and incentives for companies to respect and protect users' rights (human rights)¹.

RDR achieves this by ranking the world's most powerful digital platforms and telecommunications companies on relevant commitments and policies, based on international human rights standards. The RDR team works with companies as well as advocates, researchers, investors, and policymakers to establish and advance global standards for corporate accountability².

Paradigm Initiative works to provide digital opportunities to young Africans and promote digital rights and human rights respecting legislation and policies across Africa.

It is against this backdrop that Paradigm Initiative partnered with Ranking Digital Rights to rank telecommunications companies compliance to human rights standards in three countries; Angola, Central African Republic (CAR) and Democratic Republic of Congo (DRC) under the Greater Internet Freedom Project.

1 Ranking Digital Rights, 2021, <https://rankingdigitalrights.org/about/> (accessed 10th August 2021).

2 Ranking Digital Rights, 2021, <https://rankingdigitalrights.org/about/> (accessed 10th August 2021).

02



Country Context

Angola

Angola is a Southern African country with a population of 33 million³ (2020). Angola has three mobile phone companies, Movitel, Unitel and the state-owned Angola Telecom. In 2019, it was announced that the country would have a new operator called Africell, which is expected to launch in 2022⁴. According to HootSuite, in 2021 Internet users stood at 10 million representing a penetration of 31% of the total population. Mobile phone access stands at more than 15 million users, representing 46% of the total population⁵⁶.

In the 2020 Freedom on the Net report, Freedom House rated Angola's Internet freedom status as partly free⁷. There are no explicit government restrictions on access to the Internet and text messaging. There are no known cases of government blocking or filtering of Internet content and no known restrictions on the type of information or content that can be exchanged during communications.

3 World Bank, 2020, Angola Country Data, <https://data.worldbank.org/indicator/SP.POP.TOTL?locations=AO> (accessed 10th August 2021).

4 Africell, 2021, <https://www.africell.com/en/markets/angola> (accessed 10th August 2021).

5 Hootsuite, 2021, Digital 2021 in Angola, <https://datareportal.com/digital-in-angola>, (accessed on 20th May 2021).

6 It is important to note that the regulator INACOM does not provide up-to-date data on the use of information and communication technologies in Angola.

7 Freedom House, 2020, Freedom on the Net Report: Angola, <https://freedomhouse.org/country/angola/freedom-net/2020>, (accessed on 20 December 2021).

The Angolan Constitution⁸ provides for freedom of expression and the press, and in January 2017 a set of new media laws known as the Social Communication Legislative Package, which includes a new Press Law, Television Law, Broadcast Law, Journalists' Code of Conduct, and statutes to establish the Angolan Regulatory Body for Social Communication (Entidade Reguladora da Comunicação Social Angolana-ERCA) were enacted. The Law on Electronic Communications and Information Company Services governs the ICT and telecoms sector and provides for citizens' rights to privacy and security online.

Central African Republic

The Central African Republic (CAR) is a country in the Central African Economic and Monetary Community (CEMAC) zone located in Central Africa. In 2021, CAR had a population of approximately 4.9 million inhabitants⁹. The country has been engaged in the development of ICT infrastructure since 2020. Four operators share the mobile telephone subscriber market, namely Orange, Telecel, Moov and Azur. The Internet penetration rate is over 43.9% according to the Electronic Communications and Post Regulatory Authority (ARCEP)¹⁰. The operators offer 2G and 3G mobile service with services that cover the largest cities in the country. The Telecommunications Regulatory Agency in the Central African Republic (ART) is the institution endowed with legal personality and management autonomy in accordance with Law 07-020 of December 28, 2007. ART has been providing monitoring since 2004, ensuring technological oversight over the

application of regulations and development and promotion of the telecommunications sector as well as information and communication technologies in the country.

Democratic Republic of Congo

The Democratic Republic of the Congo (DRC) is a country in Central Africa with a population of nearly 79 million people. In DRC, the mobile telephony market is shared between four operators: Vodacom, Orange, Airtel Congo and Africell. In the second quarter of 2021, the four operators reached 44.85 million with an increased rate of 7.84%¹¹. During the same period, these companies recorded an improvement in the penetration rate of around 3.7%, that is, the penetration rate increased from 47.1% to 50.8%¹². Telephone operators operate under the new Law n° 20/017 of 25 November 2020 relating to telecommunications and information and communication technologies of 25 November 2020 in DRC under the coordination of the Congo Post and Telecommunications Authority (ARPTC). Companies' commitments in terms of freedom of expression are framed by law n° 013-2002 of October 16, 2002.

8 Constitution of Angola, Article 40

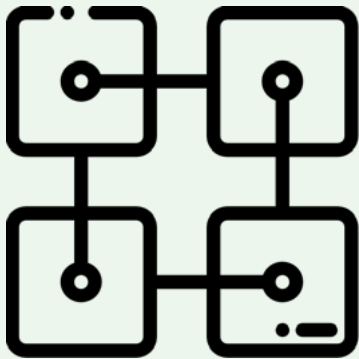
9 Country Meters, 2021, Central African Republic, https://countrymeters.info/fr/Central_African_Republic, (accessed 24 December 2021).

10 Tableau de bord marchés de télécom, 2020, https://www.arcep.cf/images/documents_divers/observatoires/2020/TAB_LEAU_DE_BORD_MARCHES_TELECOM_RCA_Q1_2020.pdf, page 17, (accessed 24 December 2021).

11 Deskeco, millions d'abonnés recensés au 2e trimestre 2021, <https://deskeco.com/2021/11/22/rdc-4485-millions-da-bonnes-actifs-recenses-la-fin-du-2e-trimestre-2021-sur-le-marche-de-la>, (accessed 24 December 2021).

12 Ibid

03



Methodology

The assessment of the telecommunications companies was conducted using the 2022 Ranking Digital Rights Corporate Accountability Index which consists of several indicators under Governance, Privacy and Freedom of Expression clusters.

Specifically, this research focused on mobile network providers that provide both data and voice services and assessed a total of 24 sub-indicators under the three clusters (Governance - 5 indicators, Freedom of Expression - 5 indicators, Privacy - 14 indicators). The following indicators were used to carry out the assessments:

Governance

- G1. Policy commitment
 - G2. Governance and management oversight
 - G4 (a). Impact assessment: Governments and regulations
 - G4 (b). Impact assessment: Processes for policy enforcement
 - G5. Stakeholder engagement and accountability
- ### **Freedom of Expression and Information**
- F1 (a). Access to terms of service
 - F3 (a). Process for terms of service enforcement
 - F9. Network management
 - F10. Network shutdown
 - F11. Identity policy

Privacy

- P1 (a). Access to privacy policies
- P3 (a). Collection of user information
- P3 (b). Inference of user information

- P4. Sharing of user information
- P5. Purpose for collecting, inferring, and sharing user information
- P6. Retention of user information
- P7. Users' control over their own user information
- P8. Users' access to their own user information
- P10 (a). Process for responding to government demands for user information
- P10 (b). Process for responding to private requests for user information
- P11 (a). Data about government demands for user information
- P11 (b). Data about private requests for user information
- P12. User notification about third-party requests for user information
- P15. Data breaches

generated containing all the findings and analyses.

The research process utilized 3 steps of the RDR research process.

Step 1: Primary Data Collection: At this step, the primary researchers collected data and sources for their assigned companies. The companies were scored based on an assessment of disclosure for every element of each indicator i.e. Full disclosure, partial disclosure, no disclosure found, no disclosure exists and not applicable. This step was crucial for providing a preliminary assessment of company performance for each indicator and element. This data was entered into input sheets customised for each company.

Step 2: Secondary Review: At this step, each of the researchers fact-checked each other's assessments under Step 1. This step was crucial for providing the necessary verification of all data collected.

Step 3: Review and Reconciliation: At this step, both researchers discussed the results from Steps 1 and 2. This step was crucial for resolving any differences and agreeing on findings. A report was

04



Rationale and limitations of the study

Angola

With the coming of a 4th mobile operator in Angola, this research sought to assess two of the existing prominent and privately owned mobile network providers which enjoy a relatively high subscribership, Movitel and Unitel. This assessment serves to highlight some of their policy provisions contained in publicly available terms of service (terms and conditions), identify gaps and provide information and advocacy points to users and civil society actors in Angola, as well as serve as a guide to new mobile operators on human rights standards and practices to prioritise and adhere to while providing safeguards and boosting users' confidence. However, there was insufficient data to support the analysis of Movitel and thus it is not included in the research findings

Central African Republic

In CAR, the mobile operators have a relatively low level of infrastructure and engagement. The research on this country aims to assess the terms and conditions of mobile operators in the country on human rights standards and practices, in order to prioritize and encourage compliance with human rights commitments, while evaluating guarantees and building user confidence. The results of this research present the level of commitment of Orange company in CAR for issues of governance, freedom of expression and privacy.

Democratic Republic of Congo

Over the past two years, two new operators have expressed their willingness to invest in the ICT market in DRC. The market is currently occupied by four operators. The objective of the research is to assess the level of commitment to respect for human rights for the operator Orange and Vodacom in order to highlight the provisions contained in the policies and conditions of service available (terms and conditions), to identify the failures and provide information and advocacy points to users and civil society actors in DRC, as well as to create internal change and serve as new challenges to the new mobile operators considering investing in the market. However, we did not have enough data to support the analysis on the company Vodacom, and it is therefore not included in the results of this research.

05



Summary of findings of the study

In general, research based on the RDR indicators shows that operators in these three countries have significant loopholes in their policies or terms of services that could promote digital rights violations. Unitel's terms and conditions are accessible on the company website and they clearly stipulate the types of content or illegal activities that may lead to user account restrictions or suspension of a service. In addition, the policy provides for dispute resolution should such a case arise.

Unitel demonstrates some good level of compliance to respect for Privacy, Freedom of Expression and Access to Information as articulated in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. However, it falls short greatly on the Governance category which analyses what governance processes are in place by management to ensure that the company respects the human rights to freedom of expression and privacy.

Unitel has a clearly articulated policy commitment to privacy, however, no explicit policy commitment to freedom of expression and access to information exists.

Unitel does not provide policy provisions that stipulate how senior leadership engage with stakeholders on human rights positions or provide oversight over the enforcement of the company's terms and human rights provisions.

Unitel does not disclose its commitments to net-neutrality or state whether it prioritises Internet traffic.

Unitel does not disclose whether it complies with government demands to shut down the Internet. There is insufficient information on data requests by the government or by private companies; neither is there disclosure on avenues for disclosing the number of demands received to restrict access to a service nor the number of cases complied with.

Unitel's sim registration terms pose a threat to the privacy of users who are required to verify their identity with their government-issued national identification card, or other forms of identification for foreign nationals that are connected to their offline identity.

Unitel clearly discloses the user information that it collects that is necessary for the provision of products or services. However, it does not specify how it collects each of the different types of user information or if this information is shared with third parties, governments or legal authorities.

Unitel's users have the power to control the collection and use of their data and are at liberty to request the company to control the collection process, delete user information and turn off targeted advertising.

Unitel does not disclose measures on retention of user information and the process for addressing data breaches.

Orange is behind in terms of information transparency on key indicators linked to the 2020 RDR indices, in particular on the protection of freedom of expression and the right to access information of its employees and users. The companies do

not have information easily exploitable by the users. The structuring of this information on the websites of national companies does not support a better ranking.

Orange's transparency report for 2020¹³ is insufficient and does not provide information on the various national companies in the world. On the global Orange Company website, we can find information about its process for handling personal data and managing privacy by the company. This information is not specifically available by each national company.

Orange does not have sufficient information on data requests by the government or by private companies; there is no stipulated application process which is a vulnerability of the way it protects the privacy and security of its users.

In general, the lack of information on human rights commitments reflects the unwillingness of the companies to better structure information on national companies.

Nevertheless, both companies have sufficient information on the mobile plans (Orange) and COVID-19 policies (Unitel).

13 Orange 2020 integrated annual report, 2020, <https://rai2020.orange.com/fr/>, (accessed 27 December 2021).

06



Company Assessments and Findings

6.1. Unitel Angola

I. Governance

Indicators in this category seek evidence that the company has governance processes in place to ensure that it respects the human rights to freedom of expression and privacy. Both rights are part of the Universal Declaration of Human Rights and are enshrined in the International Covenant on Civil and Political Rights.

G1. Policy Commitment- The company should publish a formal policy commitment to respect users' human rights to freedom of expression, access to information and privacy.

The company does in part make an explicit, clearly articulated policy commitment to human rights such as privacy, through a privacy policy, but does not make any explicit policy commitment to freedom of expression and access to information.

G2. Governance and management oversight- The company's senior leadership should exercise oversight over how its policies and practices affect freedom of expression and information, and privacy. The company does not disclose any provision for the senior leadership such as board of directors, executive level or management level committees to provide oversight over how company practices affect freedom of expression and access to information and privacy

G4 (a). Impact assessment: Governments and regulations Companies should conduct regular,

comprehensive, and credible due diligence, through robust human rights impact assessments, to identify how government regulations and policies affect freedom of expression and information and privacy, and to mitigate any risks posed by those impacts in the jurisdictions in which it operates.

The company does not disclose if it conducts regular, comprehensive, and credible due diligence, through robust human rights impact assessments in order to identify how government regulations and policies affect freedom of expression, access to information and privacy and to mitigate any risks posed by those impacts in Angola.

G4 (b). Impact assessment -: Processes for policy enforcement- The company should conduct regular, comprehensive, and credible due diligence, such as through robust human rights impact assessments, to identify how its processes for policy enforcement affect users' fundamental rights to freedom of expression and information, to privacy, and to non-discrimination, and to mitigate any risks posed by those impacts.

The company does not disclose if it conducts regular, comprehensive, and credible due diligence, such as through robust human rights impact assessments, to identify how its processes for policy enforcement affect users' fundamental rights to freedom of expression and information, to privacy, and to non-discrimination, and to mitigate any risks posed by those impacts.

G5. Stakeholder engagement and accountability- The company should engage with a range of stakeholders on the company's impact on freedom of expression and information, privacy, and potential risks of related human rights harms such as discrimination.

The company does not disclose whether or not it engages with a range of stakeholders on the company's impact on freedom of

expression, access to information, privacy and potential risks of related human rights harms such as discrimination.

II. Freedom of Expression

Indicators in this category seek evidence that the company demonstrates it respects the right to freedom of expression and access to information, as articulated in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and other international human rights instruments.

F1 (a). Access to terms of service: The company should offer terms of service that are easy to find and easy to understand.

The terms of service for the Unitel Group and local company in Angola are both available on the respective company websites and are easy to locate. Unitel Angola has the policies available in Portuguese which is the primary language in the country. The website is also fully compatible with website translation tools making it easy for someone to access the policies in their primary language.

F3 (a). Process for terms of service enforcement- The company should clearly disclose the circumstances under which it may restrict content or user accounts.

Unitel Angola's terms of service disclose the types of offences and content that are not permitted on their networks and outline circumstances in which it may suspend or restrict a user account and in part, the process for dispute resolution should such a case arise. Content such as sweepstakes, games, promotion of products and events if used for commercial exploration of the service provided by Unitel may result in suspension of a user account. In addition offences such as use of their service to provide illegal services, breach of contractual obligations, providing false declarations relating to the subscriber's identification, failure

to provide an identification document for attachment to the database and in general, any situations that may affect the proper functioning of their network, quality of service or cases that interfere with the company's interests and services. The company does not clearly disclose information about the processes it uses to identify or flag content or accounts that violate the company's rules or if any algorithmic systems are involved. However, the policy mentions the automatic processing of user information.

F9. Network management (telecommunications companies)-

The company should clearly disclose that it does not prioritize, block, or delay certain types of traffic, applications, protocols, or content for any reason beyond assuring quality of service and reliability of the network.

The company does not disclose any policy commitment to not prioritize, block, or delay certain types of traffic, applications, protocols, or content for reasons beyond assuring quality of service and reliability of the network.

F9.3. If the company does engage in network prioritization practices for reasons beyond assuring quality of service and reliability of the network, does it clearly disclose its purpose for doing so?

The company does not disclose whether or not it engages in zero-rating programs that prioritize network traffic for reasons beyond assuring quality of service and reliability of the network.

F10. Network shutdown (telecommunications companies) -

The company should clearly disclose the circumstances under which it may shut down or restrict access to the network or to specific protocols, services, or applications on the network.

The company clearly discloses that it may restrict access to the network by a user(s)

if one uses their service to provide illegal services, breach of contractual obligations, providing false declarations relating to the subscriber's identification, failure to provide an identification document for attachment to the database and in general, any situations that may affect the proper functioning of their network, quality of service or cases that interfere with the company's interests. In addition, content such as sweepstakes, games, promotion of products and events if used for commercial exploration of the service provided by Unitel is prohibited and may lead to suspension of a user's account.

F10.2. Does the company clearly disclose why it may restrict access to specific applications or protocols (e.g., VoIP, messaging) in a particular area or to a specific group of user

The company does not disclose why it may restrict access to specific applications or protocols (e.g., VoIP, messaging) in a particular area or to a specific group of users.

F10.3. Does the company clearly disclose its process for responding to government demands to shut down a network or restrict access to a service?

The company does not disclose its process for responding to government demands to shut down a network or restrict access to a service.

F10.4. Does the company clearly disclose a commitment to push back on government demands to shut down a network or restrict access to a service?

The company does not disclose any commitment to pushing back on government demands to shut down a network or restrict access to a service.

F10.5. Does the company clearly disclose that it notifies users directly

when it shuts down a network or restricts access to a service?

The company clearly discloses that it notifies the subscriber in advance when it shuts down a network or access to a service

F10.6. Does the company clearly disclose the number of network shutdown demands it receives?

The company does not disclose the number of network shutdown demands it receives.

F10.7. Does the company clearly disclose the specific legal authority that makes the demands?

The company does not disclose the specific legal authority that makes the demands to shut down a network or restrict access to a service.

F10.8. Does the company clearly disclose the number of government demands with which it complied?

The company does not disclose the number of government demands with which it complied.

F11. Identity policy -Does the company require users to verify their identity with their government-issued identification, or with other forms of identification that could be connected to their offline identity?

The company requires users to verify their identity with their government-issued national identification card, or other forms of identification, such as passports for foreign nationals, that are connected to their offline identity.

III. Privacy

P1 (a). Access to privacy policies- The company should offer privacy policies that are easy to find and easy to understand. The company does offer terms of service that are easy to locate and access on their

website, as well as presented in an easily understandable manner. The policies are presented in Portuguese, which is the primary language spoken in Angola and the webpage is fully compatible with translation tools hence making the policies accessible by non-Portuguese users.

P3 (a). Collection of user information-

The company should clearly disclose what user information it collects, and how.

The company clearly discloses what user information it collects - name, address, telephone number, e-mail and any other data of the customer necessary for the provision of products or services. There is no specification on how it collects each of the different types of user information. Under 'security of personal data' in the privacy policy, data is used only for the purposes for which it is collected.

P3 (b). Inference of user information-

The company should clearly disclose what user information it infers and how.

The company clearly discloses all the types of user information it infers based on collected user information such as name, address, telephone number or e-mail and any other relevant data. In addition Unitel clearly discloses that it limits inference of user information to what is directly relevant and necessary to accomplish the purpose of its service. However, for each type of user information Unitel infers, it does not clearly disclose how it infers that user information.

P4. Sharing of user information-

The company should clearly disclose what user information it shares and with whom.

For each type of the user information that the company collects it does not clearly disclose if, and what type of user information it shares with third parties, governments, legal authorities.

P5. Purpose for collecting, inferring, and sharing user information-

The

company should clearly disclose why it collects, infers, and shares user information.

For each type of user information that Unitel collects, it does disclose that user information is being collected and for what purpose.

P6. Retention of user information-

The company should clearly disclose how long it retains user information.

For each type of user information Unitel collects, it does not clearly disclose how long it retains that user information and this also applies to de-identified information. The company does not disclose if it de-identifies information, deletes user information when they delete their account or the timeframe in which it deletes information once the user terminates their account.

P7. Users' control over their own user information- The company should clearly disclose to users what options they have to control the company's collection, inference, retention and use of their user information.

Unitel clearly discloses the options that users have to control the company's collection, inference and use of their data. For each type of user information the company collects, the company clearly discloses if users can control the company's collection of this user information, delete this user information, if the company can attempt to infer this user information, the options to control how their user information is used for targeted advertising and that targeted advertising is off by default.

The company does not however state if it provides users with options to control how their user information is used for the development of algorithmic systems by default, or not.

P8. Users' access to their own user information- Companies should allow

users to obtain all of their user information the company holds.

The company does not clearly disclose if a user can obtain a copy of their information, what type of information they can obtain, what type of format the information is structured in, nor can they access any public facing and private information. There is no clear disclosure whether users can have access to the list of advertising audience categories which the company has assigned to them.

P10 (a). Process for responding to government demands for user information- The company should clearly disclose its process for responding to governments demands for user information.

Unitel does not clearly disclose its process for responding to non-judicial government demands, court orders or demands from foreign jurisdictions. The company does not specify the legal basis which it may comply with government demands nor does it carry out due diligence on government demands before deciding how to respond. The company does not disclose its commitment to pushing back on inappropriate or overbroad government demands nor does it set guidance on the process for implementation of government demands.

P10 (b). Process for responding to private requests for user information- The company should clearly disclose its process for responding to requests for user information that come through private processes.

The company does not clearly disclose its process for responding to requests made through private processes, the basis for complying with such requests nor does it commit to push back on inappropriate or overbroad requests made through private requests. The company does not clearly disclose if it carries out due diligence on requests made through private processes

before deciding how to respond nor does the company disclose if it provides clear guidance or examples of implementation of its process of responding to requests made through private processes.

P11 (a). Data about government demands for user information- The company should regularly publish data about government demands for user information.

Unitel does not list or publish data about government demands for user information. Data such as the number of government demands it receives by country, number of accounts affected and categories of demands is critical.

P11 (b). Data about private requests for user information- The company should regularly publish data about requests for user information that come through private processes.

Unitel does not disclose if it regularly publishes data about requests for user information that come through private processes nor does it disclose the number of requests received.

P12. User notification about third-party requests for user information-

The company should notify users to the extent legally possible when their user information has been demanded by governments and other third parties.

Unitel does not clearly disclose if it notifies users when third parties such as government entities (including courts or other judicial bodies) and private entities demand their user information

P15. Data breaches- The company should publicly disclose information about its processes for responding to data breaches.

Unitel does not clearly disclose if it will notify the relevant authorities without undue delay when a data breach occurs, the process for notifying data subjects who might be affected by a data breach

and the steps it will take to address the impact of a data breach on its users.

6.1.1. Analysis of Unitel Angola

This section presents evidence that the company demonstrates some level of compliance to respect for Privacy and Freedom of Expression and access to Information, as articulated in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and other international human rights instruments, however, falling short greatly on the Governance category.

I. Governance

Unitel Angola has a clearly articulated policy commitment to privacy, through the company's privacy policy however, the company does not make any explicit policy commitment to freedom of expression and access to information.

No policy provision exists that stipulates how senior leadership such as the board of directors, executive-level or management-level committees should provide oversight of the enforcement of the company's terms and human rights provisions. In addition, there is no provision for carrying out regular and comprehensive human rights impact assessments of government regulations and company policies, and how these may impact user's fundamental human rights such as freedom of expression and privacy.

In terms of stakeholder engagement and accountability, the company does not provide information on whether stakeholder engagements are sought to highlight the company's impact and influence on freedom of expression and information, privacy, and potential risks of related human rights harms such as discrimination.

II. Freedom of Expression

Unitel Angola's terms of service are provided and accessible on the company

website in Angola's primary language – Portuguese. The website is also fully compatible with website translation tools making the terms accessible to a wider audience beyond Portuguese-speaking users. In terms of content and user account restrictions, the company clearly stipulates that content such as sweepstakes, games, promotion of products and events if used for commercial exploration of the service may result in the suspension of a user's account or removal of content. It is also an offence to use their service to provide illegal services, breach contractual obligations, provide false declarations relating to the subscriber's identification for sim card registration, failure to provide an identification document for attachment to the database and in general, any situations that may affect the proper functioning of their network, quality of service or cases that interfere with the company's interests. According to the policy, subscribers receive prior notice when access to the service is restricted due to misconduct.

Furthermore, a process for dispute resolution is outlined, in part, should a case of account or service suspension arise with a dedicated email contact provided for further communication and appeals.

The company does not clearly disclose information about the processes it uses to identify and flag content or accounts that violate the company's rules or if any algorithmic systems are involved, however, the terms of service state that user information is automatically processed.

Users are required to verify their identity with their government-issued national identification card, or other forms of identification and passports (for foreign nationals) that are connected to their offline identity which poses threats to personal data protection and privacy as personal information could easily be shared upon demand to government and private agencies, as well as be used to facilitate

illegal interception of communications in the case of at-risk individuals.

Unitel Angola does not disclose its commitments to net-neutrality by clearly stating that it does not prioritize, block, or delay certain types of traffic, applications, protocols, or content or VoIP messaging for any reason.

In terms of compliance to network shutdown demands by government or private sector, the company does not provide clear disclosure neither does it have avenues for disclosing the number of demands received to restrict access to a service nor the number of cases complied with.

III. Privacy

Of all of Unitel Angola's terms of service, the privacy policy is well articulated and easy to locate and access on the company website, as well as presented in an easily understandable manner. The policies are presented in Portuguese, which is the primary language spoken in Angola and the webpage is fully compatible with translation tools hence making the policies accessible by non-Portuguese users.

The company clearly discloses the user information that it collects such as name, address, telephone number, e-mail and any other data of the customer necessary for the provision of products or services, however, it does not specify how it collects each of the different types of user information and partially discloses that it limits collection of information that is directly relevant and necessary to accomplish the purpose of its service. For each type of the user information that the company collects it does not disclose if, and what type of user information it shares with third parties, governments, legal authorities. However, under the freedom of expression cluster, no information is available on whether Unitel complies with government or private sector demands for user information.

Users have the power to control the

company's collection, inference and use of their data. For all user information collected, users can approach the company requesting to control the collection process, delete user information and turn off targeted advertising although by default, all targeted advertising is off. No disclosure and options exist to control how user information is used for the development of algorithmic systems by default, or not.

No disclosure exists on retention of user information, user access to their information that the company holds, data breaches, process or responding to non-judicial, private, government and how or whether third party requests for user information are processed or published.

6.2. Orange DRC

Orange DRC is the only operator whose website contains information relevant to this report. The following indicators were used to carry out the research.

I. Governance

G1. Policy commitment

The G1 governance indicator specifies that the company must formally publish a political commitment to respect users' human rights to freedom of expression and information and to privacy. In the terms of use of Orange DRC, no provision on respect for human commitments is indicated. The Orange parent company and Orange DRC provide no information on the commitment to human rights, including freedom of expression and access to information, and the protection of online privacy.

G2. Governance and management control

This indicator indicates that the company's top management needs to exercise control over how its policies and practices affect freedom of expression and access to information, and confidentiality.

Orange and Orange DRC do not clearly disclose whether the board of directors

exercises formal control over how company practices affect freedom of expression and information and how company practices affect confidentiality. Orange does not disclose whether the company has a committee, team, or program which oversees how company practices affect freedom of expression and access to information.

Orange does not disclose whether any executive-level committee or manager, team, program or oversees how company practices affect privacy.

Orange does not disclose whether it has an executive committee, team, or program responsible for overseeing how corporate practices affect freedom of expression and information and also how practices affect employee privacy or clients.

G4 (a). Impact assessment: governments and regulations

Indicator 4 mentions that companies should perform regular, comprehensive and credible due diligence, through robust human rights impact assessments, to identify how government regulations and policies affect freedom of expression, information and confidentiality, and to mitigate the risks posed by these impacts in the jurisdictions in which it operates.

Orange does not present any information about how the laws affect freedom of expression and information in jurisdictions in the DRC.

Orange DRC does not say how the laws affect privacy in the jurisdictions in which it operates.

Orange does not inform users or customers of any risk related to freedom of expression and information associated with existing products and services in the jurisdictions in which it operates.

Orange does not have a process for the privacy risks associated with existing products and services in the jurisdictions in which it operates.

Orange has no provision on the risks related to freedom of expression and information associated with a new activity,

including the launch and/or acquisition of new products, services or businesses, or entry into new markets or jurisdictions.

Orange does not have a provision that assesses the privacy risks associated with a new activity, including the launch and or acquisition of new products, services or businesses, or entry into new markets or jurisdictions.

Orange does not perform an additional assessment every time the company performs risk assessments and identifies problems.

Orange does not define a mechanism for senior management and or members of the company's board of directors to review the results of assessments and due diligence in their decision-making. No evaluation schedule is available.

Finally, for this indicator, Orange does not have a third-party committee for external evaluations, nor information on an external third-party committee responsible for evaluations and accredited according to a relevant human rights standard and reputed by a credible organization.

G4 (b). Impact assessment: policy implementation process

This indicator specifies that the company should perform regular, comprehensive and credible due diligence, for example, through robust human rights impact assessments, to determine how its policy enforcement processes affect users' fundamental rights to freedom of movement, expression and information, privacy and non-discrimination, and mitigate the risks posed by these impacts. Orange in its operation does not assess the risks related to freedom of expression and information related to the application of its conditions of use.

The company does not conduct risk assessments related to the application of its privacy policies, nor does it assess the risks of discrimination related to its processes for applying its terms of service. The risks of discrimination associated with the process of applying its privacy

policies are not assessed. No additional assessment whenever business risk assessments identify issues are undertaken by the business.

Senior executives and/or members of the board of directors of the company do not participate in the review of evaluation results and due diligence in their decision-making. No evaluation schedule is indicated and the company does not perform evaluations provided by a committee of third parties to ensure developments according to a relevant human rights standard and reputed by a credible organization.

G5. Stakeholder engagement and accountability

This indicator shows that the company should engage with a range of stakeholders on the company's impact on freedom of expression and information, privacy, and potential risks of related human rights harms such as discrimination.

The company doesn't have a member of one or more multi-stakeholder initiatives that address the full range of ways in which users' fundamental rights to freedom of expression and information, privacy, and non-discrimination may be affected in the course of the company's operations.

The company doesn't have a member of one or more such multi-stakeholder initiatives, and the company doesn't have a member of any organizations that engage systematically and on a regular basis with non-industry and non-governmental stakeholders on freedom of expression and privacy issues.

The company does not disclose whether it initiates or participates in meetings with stakeholders who represent, defend individuals whose rights to freedom of expression and information and to privacy are directly impacted by the activity of the company.

II. Freedom of Expression

F1 (a). Access to terms of service

The company should offer terms of

service that are easy to find and easy to understand.

Orange's terms of service are easy to find. They can be found at the bottom of the home page.

Also, the terms of service are available in the primary language(s) spoken by users in the company's home jurisdiction. The website could be easily translated from English to French.

The terms of service presented are not easily understandable. The provisions and structuring of the terms of service do not facilitate research.

F3 (a). Process for terms of service enforcement

The company should clearly disclose the circumstances under which it may restrict content or user accounts.

The company clearly discloses what types of content or activities it does not permit. Section 4 on the Orange SIM card policy, mentions how the company interacts with content.

The company clearly discloses why it may restrict a user's account in section 4 of the terms and conditions.

Also in section 4, the company partially discloses information about the processes it uses to identify content or accounts that violate the company's rules. Information about this element is not clear.

Therefore, the company doesn't clearly disclose how it uses algorithmic systems to flag content that might violate the company's rules.

The company doesn't clearly disclose whether any government authorities receive priority consideration when flagging content to be restricted for violating the company's rules.

F9. Network management

The company should clearly disclose that it does not prioritize, block, or delay certain types of traffic, applications, protocols, or content for any reason beyond assuring quality of service and reliability of the network.

The company does not prioritize clearly, block, or delay certain types of traffic, applications, protocols, or content for any reason beyond assuring quality of service and reliability of the network.

The company doesn't clearly disclose a policy commitment to not prioritize, block, or delay certain types of traffic, applications, protocols, or content for reasons beyond assuring quality of service and reliability of the network.

The company doesn't engage in practices, such as offering zero-rating programs that prioritize network traffic for reasons beyond assuring quality of service and reliability of the network.

The company doesn't engage in network prioritization practices for reasons beyond assuring quality of service and reliability of the network, it clearly discloses its purpose for doing so.

F10. Network shutdown

F10.2. Does the company clearly disclose why it may restrict access to specific applications or protocols (e.g., VoIP, messaging) in a particular area or to a specific group of user

No disclosure found. The company doesn't clearly disclose the circumstances under which it may shut down or restrict access to the network or to specific protocols, services, or applications on the network.

F10.3. Does the company clearly disclose its process for responding to government demands to shut down a network or restrict access to a service?

The company doesn't clearly disclose the reasons why it may shut down service to a particular area or group of users. The company doesn't clearly disclose why it may restrict access to specific applications or protocols (e.g., VoIP, messaging) in a particular area or to a specific group of users.

F10.4. Does the company clearly disclose a commitment to push back on government demands to shut down a network or restrict access to a service?

The company doesn't clearly disclose a commitment to push back on government demands to shut down a network or restrict access to a service.

F10.5. Does the company clearly disclose that it notifies users directly when it shuts down a network or restricts access to a service?

The company doesn't clearly disclose that it notifies users directly when it shuts down a network or restricts access to a service.

F10.6. Does the company clearly disclose the number of network shutdown demands it receives?

The company does not disclose the number of network shutdown demands it receives. The company doesn't clearly disclose the number of network shutdown demands it receives.

F10.7. Does the company clearly disclose the specific legal authority that makes the demands?

The company doesn't clearly disclose the specific legal authority that makes the demands.

F10.8. Does the company clearly disclose the number of government demands with which it complied?

The company doesn't clearly disclose the number of government demands with which it complied.

F11. Identity policy -Does the company require users to verify their identity with their government-issued identification, or with other forms of identification that could be connected to their offline identity?

The company requires users to verify their identity with their government-

issued identification, or with other forms of identification that could be connected to their offline identity.

The company should not require users to verify their identity with their government-issued identification, or other forms of identification that could be connected to their offline identity.

The conditions specify that the user must give his name, middle name and/or first name, physical address, nationality, place and date of birth, type and number of the identity document.

III. Privacy

P1 (a). Access to privacy policies

The company offers privacy policies that are easy to find and easy to understand for prepaid mobile. No disclosure found for post-paid mobile.

The company's privacy policies are easy to find. The privacy policies can be found in terms and conditions on the home page. The privacy policies are available in the primary languages spoken by users in the company's jurisdiction. These policies are presented in an understandable manner.

P3 (a). Collection of user information

The company should clearly disclose what user information it collects and how.

The company clearly discloses what types of user information it collects.

The company doesn't clearly disclose how it collects user information.

The company partially discloses that it limits collection of user information to what is directly relevant and necessary to accomplish the purpose of its service.

P3 (b). Inference of user information

The company should clearly disclose what user information it infers and how.

The company clearly discloses all the types of user information it infers on the basis of collected user information.

For each type of user information the company infers, the company clearly discloses how it infers that user information.

The company clearly discloses that it limits inference of user information to what is directly relevant and necessary to accomplish the purpose of its service.

P4. Sharing of user information

The company should clearly disclose what user information it shares and with whom. For each type of user information the company collects, the company clearly discloses whether it shares that user information.

For each type of user information the company shares, the company clearly discloses the types of third parties with which it shares that user information.

No disclosure found that the company clearly discloses that it may share user information with government(s) or legal authorities.

No disclosure found for each type of user information the company shares, nor clearly discloses the names of all third parties with which it shares user information.

P5. Purpose for collecting, inferring, and sharing user information

The company should clearly disclose why it collects, infers, and shares user information.

No disclosure found for how the company collects each type of user information.

No disclosure found for how the company intersects with each type of user information the company infers, and clearly disclose its purpose for the inference.

No disclosure found for how the company disclose whether it combines user information from various company services and if so, why?

No disclosure found for how each type of user information the company shares, and if the company clearly discloses its purpose for sharing.

The company doesn't clearly disclose that it limits its use of user information to the purpose for which it was collected or inferred.

P6. Retention of user information

The company should clearly disclose how long it retains user information. But, no disclosure was found for elements of privacy and retention of user information. The company partially discloses that it deletes all user information after users terminate their accounts.

The company doesn't clearly disclose the time frame in which it will delete user information after users terminate their accounts.

P7. Users' control over their own user information

The company doesn't clearly disclose to users what options they have to control the company's collection, inference, retention and use of their user information. No disclosure found for all elements in users' control.

P8. Users' access to their own user information

Companies should allow users to obtain all of their user information the company holds.

The company clearly discloses that users can obtain a copy of their user information. The company doesn't clearly disclose what user information users can obtain.

No disclosure found for elements on users' access to their own user information for subsections.

P10 (a). Process for responding to government demands for user information

The company doesn't clearly disclose its process for responding to governments demands for user information. No disclosure found for all elements.

P10 (b). Process for responding to private requests for user information

The company doesn't clearly disclose its process for responding to requests for user information that come through private processes. No disclosure found for

all elements.

P11 (a). Data about government demands for user information

The company doesn't regularly publish data about government demands for user information. No disclosure found for all elements

P11 (b). Data about private requests for user information

The company doesn't regularly publish data about requests for user information that come through private processes. No disclosure found for all elements.

P12. User notification about third-party requests for user information

The company doesn't notify users of the extent legally possible when their user information has been demanded by governments and other third parties. No disclosure found for all elements.

P15. Data breaches

The company doesn't publicly disclose information about its processes for responding to data breaches. No disclosure found for all elements.

6.2.1. Analysis of Orange DRC-CAR

The Orange company in DRC obtains a higher score than CAR. These scores differ due to the lack of information on the company's website in CAR. In general, information on the actual level of Orange commitment in the DRC and CAR is very low. The data available to enable the level of engagement of national companies to be assessed based on governance, freedom of expression and protection of privacy indices are also weak. In DRC, for the past 5 years, the government has ordered the company to shut down Internet connection or network during political operations. These same practices are also noticeable in CAR. Orange DRC

and CAR perform poorly on our research indicators measuring various issues related to network governance, freedom of expression and information on privacy.

I. Governance

The Orange¹⁴ parent company has a good score on governance. The governance indicator remains unavailable for national companies and difficult to interpret because the company does not have information based on the context and laws of each country.

Commitment in favour of human rights: Orange companies in DRC and CAR do not have explicit information which commits companies to respect the freedom of expression and the right to privacy of users. Although senior management of the company exists to exercise oversight over how its policies and practices affect freedom of expression and information, and confidentiality, no transparency information for national companies in DRC and CAR are available.

Human rights due diligence: Orange partially provides information on how to conduct solid human rights impact assessments. Unfortunately, Orange DRC and CAR do not disclose information about these national companies on how laws and regulations affect freedom of expression and privacy in these distinct markets. Also, the company does not disclose information about conducting similar reviews of terms and conditions of use, local advertising data, and other applications.

Stakeholder engagement: The Orange parent company is a member of the Global Network Initiative, a multi-stakeholder organisation whose dual purpose is to prevent internet censorship by authoritarian governments and to protect the privacy rights of individuals

14 Orange, 2021, <https://www.orange.com/fr>, (accessed 27 December 2021).

on the internet. However, the company does not have enough information on the benefits and demands of government and third-party companies that Internet users face in relation to human rights.

II. Freedom of Expression

Orange in the DRC and CAR is visibly low in terms of data analysis on freedom of expression issues, but try to improve this by putting in place new laws, as well as new ICT frameworks that respect user rights and respect human rights.

Control, content blocking and account suspensions: Orange's terms of service are available and easy to find, but they have little information to better understand all of Orange's commitments at the local level. Also, the company has not disclosed any data detailing how it is implementing the rules, such as blocking content or suspending accounts in both countries.

Content and advertising targeting: Orange has not published any relevant information on the rules governing advertising content and targeting on its services or on how these rules are applied. Network management: Orange has no information on the network management process, whether at the parent-company level or at national companies' level in DRC and CAR. As noted in Orange company previous reports on network management, it has still not made a clear commitment to net-neutrality, nor revealed whether it engages in practices that prioritize network traffic, such as network zero-rating programs. In reference to network shutdowns, the company does not clearly disclose the circumstances under which it may shut down or restrict access to the network or to specific protocols, services, or applications on the network. With regards to Identity Policy, the company has information that allows users to verify their identity with their government-issued ID or other forms of identification that could be linked to their offline identity.

III. Privacy

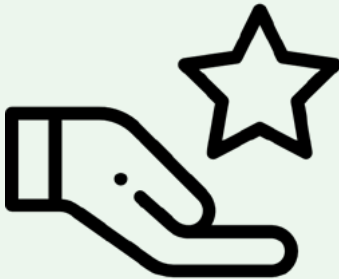
Orange seems to have made more progress in managing user privacy.

Processing of user data: Orange has a clear and accessible Privacy Policy. This policy applies to parent and local companies. The company also discloses how user data is collected. The Orange company clarifies the types of data it collects but provides inconsistent details on the data collection process. Unfortunately, the company hasn't released anything on the types of data it inferred. On the issue of sharing user information, the company has made clear what user information it shares but does not have sufficient information about the third parties with whom it shares. Orange does not clearly disclose why it collects and infers information, or how it shares user information. Orange's privacy policy does not disclose how users can object to certain uses of the information and delete it. Users do not have access to all information, but privacy policies for the Orange parent company specify that they can change it as they wish without details of the procedure.

Government and private requests for user data: Orange does not have sufficiently clear information on requests for third-party user data from all telecommunications companies in relation to local jurisdictions, nor on the management process. Orange does not disclose information on private requests for user data by governments.

Data security and control: Parent or national Orange companies do not disclose whether the company should notify users of the extent permitted by law when user information is requested by governments and other third parties. Also, the company does not disclose anything about how it handles personal data breaches in the event of forced or wilful intrusion.

07



Recommendations

In order to improve the level of engagement, national companies and the Orange parent company must make the following commitments:

7.1. Unitel- Angola 🇦🇴

Through its terms of service Unitel must improve reporting transparency by providing the necessary and complete policies and information on the company's governance structures and commitment to safeguarding freedom of expression and privacy.

Unitel must continuously engage in human rights impact assessments and conduct significant human rights impact studies of its services and use the results to inform their terms of services and operations.

Unitel should enhance its data management by indicating how the company uses the data for advertising and what privacy measures are in place for data that is collected for the purpose of sim card registration and tied to user's offline identities.

Unitel must highlight the process for data retention and addressing data breaches.

Unitel should disclose whether it complies with government demands to shut down the internet or on data requests by the 🇦🇴 government or by private companies, and go on further to disclose the number of cases complied with within a given period.

7.2. Orange-CAR/DRC

Orange should commit to providing the necessary and complete information on governance, freedom

of expression and privacy. Orange should also commit to information transparency on platforms. Orange should structure information on governance, freedom of expression and privacy by country, taking into account the relevant national laws.

Orange should improve reporting transparency. Orange should publish reports on each specific country to share information on the way therefore governance, freedom of information and data management are carried out after a given period.

Orange should engage in human rights impact assessment based on company terms of conditions. Orange should conduct significant human rights impact studies of its services by country and draw up an impact result.

Orange should improve data management for advertising purposes. Orange should indicate which companies use the data for advertising purposes and how users can unsubscribe.

Orange should promote transparency and human rights regarding the use of information collected through automated forms.

Orange should promote transparency in the process of responding to government calls for Internet disruptions.

Orange should share information on the network management process.

Orange should improve reporting transparency by providing the basic and complete policies, and information on the company's governance structures and commitment to safeguarding freedom of expression and privacy.

Orange should promote transparency and clear information on requests for third party user data from all telecommunications

companies and in relation to local jurisdictions.

