Privacy / Data protection Law:

How much disclosure does growth need?

Africa 2.0: A brave new (digital) world

Annual Conference of the African Bar Association

Port-Harcourt, Nigeria

6 – 10 August 2017

MIRANDA

Miranda & Associados Sociedade de Advogados RL

CONTENTS

TITLE

Abstract

It is unquestionable that, in recent years, Africa has been living an increasing fast speed digital transformation process. Such transformation translates not only in the use of new and more sophisticated technologies by both public and private entities but also in the enactment of new statutes and other relevant pieces of legislation.

The digital world is however not without its faults and, as knowledge – and data – become more easily accessible, so too is easier for abuses and lack of accountability to take place. One of the most vulnerable and, at the same time, important areas to be affected is that of privacy and personal data.

Either by choice of the data subjects (which many times unwillingly or not fully informed on the risks or purposes of processing divulge their own personal data in the digital world) or by means of external impositions (such as having a professional e-mail account where data is possibly stored in unsecured ways), personal data is an easy commodity to gamble without often considering the actual cost of such actions. On the other hand, data privacy cannot and should not be a tool to promote money laundering, corruption and nepotism.

It is thus the purpose of this paper to analyze the current legal framework in certain African countries from a somewhat regional perspective at the same time as it seeks to present some suggestions of conceivable solutions for future implementation across Africa. The future of data protection in Africa will have to take into account the speed at which African countries are reducing their digital potential towards the most developed countries, learn from the bad experiences of other more developed countries and understand the pace at which the world is transforming from a technology standpoint, where Artificial Intelligence will change a significant number of our current paradigms. Therefore, this paper seeks to address some of the main showstoppers to be considered from a legal and regulatory standpoint and which are the most advisable courses of action. We will also discuss the impact of the new General Data Protection Regulation ("GDPR") as a possible new international standard.

Having privacy and data protection as core areas of observation, this paper debates issues such as data localization and cross-border transfer of data from a comparative perspective, taking into account systems that have a successful track-record of protecting privacy at the same time as it does not overlook Africa as a complex reality and its own singularities.

Keywords: Personal data; Privacy; African legal systems; Disclosure of personal data

1. Introduction – One continent, many realities

Every day, a huge amount of personal data is being illicitly processed, i.e. it is being processed in a way that does not respect either national or international data protection regulations.

As new technologies became more and more common in every citizens' life, where the relevant servers collecting and processing data are located anywhere in the world, the need to adopt effective regulations and agreements became even cleared as it was the only way to control the (un)controllable.

It is however well-known that Africa is still taking its first steps on the effective protection of personal data and of its citizens' privacy. This can be proven to be an exceptional difficult challenge on the world's second largest continent in terms of size and population.

Unlike what happens in the European Union (hereinafter "EU"), African countries still have sufficient autonomy to adopt (or not) unique approaches when it comes to the enactment and enforcement of privacy and data protection legislation. To put it differently, *"despite the emerging data privacy policies in the continent, there is yet no philosophical conception of the term privacy in the African context"*.[1]

On a World where international data flows are not a commodity but, more and more, a necessary currency and working tool, such autonomy can prove to have adverse effects, as *"countries which refuse to adopt meaningful privacy laws may find themselves unable to conduct certain types of information flows with Europe"*[2] as well as with other regions of the globe.

Be that as it may, we are able to find an increasing effort at a regional level at creating some type of benchmark which can be used as a reference in the different countries. By means of example, the African Union ("AU") have adopted on 27 June 2014, the AU Convention on Cybersecurity and Personal Data Protection in 2014. More recently, given the unremitting development of new and improved versions of the digital world, the AU also set down a set of guidelines for Internet Infrastructure Security for Africa, hoping to reach this same regional unified goal.

---

[1] A. B. Makulilo, "The Context of Data Privacy in Africa" in *African Data Privacy Laws*, Springer International Publishing AG, 2016, p. 16

[2] Ibid.

Furthermore, we are also able to find some traces of European inspiration and, specifically, of the 95 Data Protection Directive, on the laws enacted in some countries, notably, Angola, Cape Verde and Mozambique, amongst others[3].

It is with the aforementioned examples at hand that we will try not only to map the existing legal and regulatory framework but also to anticipate the next moves that the legislator will take not only at a national but also at a regional level.

2. The current legal and regulatory landscape

2.1 Protection at a Constitutional Level – Some examples

2.1.1 Mozambique

Mozambique was chosen as the first of three examples of the African legal system as it is still to implement a data protection comprehensive regime[4].

Nonetheless, Mozambique can still provide for some degree of legal protection in data protection related issues by resorting to the country's legal provisions on privacy and protection of private life set forth in the Constitution[5].

Pursuant to Article 41 of the Constitution, all individuals are entitled to the intimacy of their private life. Further, Article 71 of the Constitution grants all individuals the right to privacy, prohibiting the use of electronic means for recording and processing individually identifiable data in respect of political, philosophical or ideological beliefs, of religious faith, party or trade union affiliation or private lives. Access to data bases or to computerized archives, files and records for obtaining information on the personal data of third parties, as well as the transfer of personal data from one computerized file to another that belongs to a distinct service or institution, shall be prohibited except in cases provided for by law or by judicial decision.

---

[3] By means of example, similar data protection laws were also enacted in countries such as São Tomé and Príncipe, Equatorial Guinea and Gabon.

[4] A closer look at the Mozambican legal regime on data protection matters can be found at Traça, João Luís; Neves, Lídia "Data Protection in Mozambique: Inception Phase" in *African Data Privacy Laws*, Springer International Publishing AG, 2016, p. 363 - 370.

[5] Additional protections can equally be found in Mozambique's civil and labor laws. More to the point, under Article 80 of the Civil Code (Administrative Ordinance no. 22869 of 4 September 1967), all individuals are required to respect the intimacy of the private life of others. Also, Mozambique has specific legal provisions that regulate the disclosure of personal data, such as Article 6 of the Labor Law (Law no. 23/2007 of 1 August 2007). This provision ensures the protection of employee's personal data, prohibiting the transfer of any private data obtained by an employer subject to a duty of confidentiality to third parties without the employee's consent, as well as of any other information which would breach the employee's privacy. The right to privacy is deemed to include all information of a personal nature in electronic format.

The Constitution also provides that all individuals shall be entitled to have access to collected data and have the same rectified. Although the Constitution does not set forth the specific information to be provided, we are of the opinion that provision of information such as details of personal data belonging to a specific individual that are being processed and information on the purposes of the processing may not be declined.

The Constitution does not define the right to rectification of collected data either. Nonetheless, an individual should be entitled to demand the correction and updating of inaccurate, incomplete, or wrong personal data. It is important to underline however that the Constitution does not provide any additional guidance on either timeframes or procedures to adopt in case these data have already been shared with third parties.

It is important to underline however that, in addition to general principles laid down in the Constitution, whenever a data controller is processing personal data within certain fields, it should also abide with an additional set of rules. Notably, both the country's labor law and Law 3/2017, of January 9th, 2017 (the "Electronic Transactions Act" or "ETC") seek to regulate how (and to what extend) can personal data be processed.

Furthermore, a special mention must be equally made to Law 34/2014, of December 31st, 2014. This statute is a ground-breaking moment from a legislative standpoint as it defined, for the first time, personal data. As such, personal data is now defined in Mozambique as any information that allows for natural persons to be identified or identifiable, regardless of such information being registered manually or electronically.

2.1.2. Angola

Unlike Mozambique, Angola has enacted a specific regime covering data processing operations in the country, by means of Maw No. 22/11, of 17 June 2011 (the "Data Protection Act")[6].

Nonetheless, before the Data Protection Act, personal data protection matters in Angola were already governed by a few constitutional and statutory provisions establishing general rights and prohibitions relating to the protection of private life and personal data.

More to the point, Article 69 of the Angolan Constitution sets out a right for any person to access computerized data that relates to him or her, enforceable by means of a writ of *habeas data*. A person bringing an action for *habeas data* can additionally demand

[6] A closer look at the Angolan legal regime on data protection matters can be found at Traça, João Luís; Correia, Francisca "Data Protection in Angola" in *African Data Privacy Laws*, Springer International Publishing AG, 2016, p. 349 - 362

that such data be corrected or updated. The *habeas data* has not been further regulated in Angolan laws and the Data Protection Act contains no reference to it.

All these rights exist both in the scope of the Data Protection Act and in the scope of Angolan constitutional rights generally. An important aspect to underline is that, while the Angolan Data Protection Act may not apply to a foreign entity, constitutional rights belong to citizens at all times, and an Angolan court or the Data Protection Agency may therefore find that, for reasons of public policy or public order, these rights cannot be excluded or avoided due to the fact that the party controlling their data does not have any type of presence in Angola.

The aforementioned idea is of particular relevance as it shows a supra-legislative concern of protecting privacy in the country at the same time as it has demonstrate a common framework with that of Mozambique (and of other African countries).

2.1.3. Cape Verde

Looking now at the Cape Verdean example, we are able to differentiate three separate provisions regulating citizens' personal data as well as privacy in the Constitution (i.e. Constitutional Law No. 1/VII/2010), in addition to the country own data protection legal regime[7].[8]

The first rule that must be underlined in connection to our subject is set down in Article 44. This provision sets down a prohibition to violate correspondence and telecommunications, thus guaranteeing the protection of all citizens' correspondence and telecommunications. Notwithstanding this fact, Article 44 allows for an "escape valve" as it states that whenever a valid judicial order is in place, public authorities may be entitled to restrict said principle thus gaining access to selected correspondence and telecommunications.

Unfortunately, the relevant provision provides very little additional guidance for what exactly constitute the abovementioned restriction. As such, due to the lack of any case law or other type of precedent on this matter, it is not possible to clearly draw a line in what exactly are the powers (and limits) that public authorities have (and must respect) whenever they enforce this constitutional provision.

---

[7] A comprehensive data protection regime was enacted in country, by means of Law No. 133/V/2001, of 22 January 2001 (as recently amended by Law No. 41/VIII/2013) the legal framework for data protection matters.

[8] A closer look at the Cape Verdean legal regime on data protection matters can be found at Traça, João Luís; Gaspar, Pedro Marques "Data Protection in Cape Verde: An Analysis of the State of the Art" in *African Data Privacy Laws*, Springer International Publishing AG, 2016, p. 249 – 258.

In addition to Article 44, the Cape Verdean Constitution equally sets down rules regarding informatics' usage and data protection. More to the point, Article 45 (1) expressly grants citizens the right to access, to correct and to update any data processed by informatics' means at the same time that it entitles citizens to know the purposes for which their data is being processed, according to the law.

Article 45 also addresses the issue of sensitive data (regardless of not specifically using the expression "sensitive data") by setting down a general prohibition to use informatics' means to process any data relating to a person's philosophical, ideological or political convictions; party or union affiliation; religious faith or private life. Said prohibition is only overcome if (i) the data subject's consent is expressly obtained; (ii) there is a legal rule specifically granting said authorization, provided that non-discrimination guarantees are in place; or (iii) the data is processed for statistical purposes in a non-identifiable way.

Practically speaking, by placing the referred to requirements to process sensitive data directly in the Constitution text, Cape Verde is taking an important (and very singular) approach to data protection matter, placing it on the level of many other countries with more mature privacy regimes.

Article 45 further creates additional limitations to protect Cape Verdean citizens. Namely, except whenever provided by law, public entities are not entitled to access to any and all files, electronic records or data bases containing personal data. Said prohibition is also applicable to the transfer of said information from one service or institution to another. Likewise, it is expressly forbidden for the Government to attribute a uniform identification number to national citizens.

Interestingly enough, and although all the referred to rules are intended to computerized means / informatics, the legislator creates a special provision stating that said principles are equally applicable to personal data stored and otherwise processed in manual files.

Meanwhile, a brief reference can be equally made to the country's concern in addressing the issue of *habeas data*, as it occurs in Angola and some other African jurisdictions. In Cape Verde, citizens are thus entitled to request, update or even to destruct any personal data by means of this writ.[9]

[9] It is important to underline that the specifics of habeas data are not found in the Constitution but in Law No. 109/IV/94, a statute which sets forth the purposes and conditions in which a party may bring an action for *habeas data*.

2.2. Comprehensive data protection Laws

As Mozambique still does not have a full regime for data protection matters, we will base our analysis at this point with the Angolan and Cape Verdean examples.

The choice of the aforementioned two jurisdictions is purely incidental as they mirror the same general principles found in other African legal regimes at the same time as they present two different stages of evolution – the case in Angola where there is a regime but the regulator is still to be fully operational and the case in Cape Verde where the legal regime is already being enforced by a local Data Protection Agency with powers to oversee and enforce the application of the law.

Looking at the general principles that can be found in both jurisdictions, the fundamental ideas to retain are as follows:

1. Data subjects have several information rights

Both in Angola and Cape Verde, the respective data protection laws grant data subjects the right to access, correct and delete any personal data relating to them. As such, data controllers must provide data subjects with free and easy means of exercising these rights.

Data controllers are under a further duty to provide data subjects, upon request, with additional information such as the purposes for which the personal data are being used, and the identity of any third parties to whom the data may be transferred, among others.

2. Data subjects' consent is necessary and data subjects have the right to oppose to the processing

As a rule and similarly to what is set down in the 95 Data Protection Directive, personal data may only be processed if the data subject has unambiguously given his/her consent.

Nevertheless, in both jurisdictions, the data subject's consent will not be required if the processing is necessary:

(i) for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract or a declaration of his/her will to negotiate;

(ii) to comply with a legal obligation to which the data controller is subject;

(iii) in order to protect the vital interests of the data subject if the latter is physically or legally not able of giving his/her consent;

(iv) for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller or in a third party to whom the data are disclosed.

3. It is necessary to respect formalities with the local regulators to ensure compliance with the relevant data protection operations

Following a rule pursuant to which data processing operations can only be initiated after making a filing with the local regulators. Angola and Cape Verde have almost identical regimes in this matter. As such, in both countries, it is necessary to conduct a filing or, if dealing with sensitive data, to request a prior authorization from the local data protection agencies.

This point is particularly interesting as the rationale behind informing the regulator is creating a second layer of protection of the data subjects. As such, the regulator can see if the data protection operations are following a correct application of the law and, if that proves not to be the case, act accordingly (namely, by prohibiting illegal processing activities).

Nonetheless, as previously stated, Angola does not have a data protection agency operating yet. Thus, it is impossible to comply at this date with any requirements directly related to it, which creates a certain degree of insecurity when conducting data protection operations.

We are the opinion however that, similarly to what occurred in Cape Verde (the Cape Verdean regulator issued more than 150 authorizations in 2016 alone, quickly rectifying any shortcomings that might have occurred prior of the setting up of the relevant agency) the situation in Angola will be easily rectified.

4. Both countries have specific rules on international transfer of personal data

Both Angola and Cape Verde set down that international transfer of personal data is only permitted if the recipient country is considered to have a sufficient level of protection regarding personal data processing matters.

Said level of protection of foreign countries is defined by the local data protection agencies. As Angola still does not have a regulator, in Angola, to the present date, there is no list of countries which fulfil this condition.

As a general rule, transfer of personal data to countries that do not provide for an adequate level of protection of personal data in both countries can only be permitted if the data subject has given his consent and if the relevant authorization has been obtained.

In Angola this could, in theory, block cross-border transfers of data. The reality of today's World makes it however impossible for international transfers to be fully obstructed. Consequently, they have to be based solely in the data subjects' consent (which might sometimes be deemed not sufficient if we look at the strict wording of the law). Furthermore, one can always challenge if there is an effective consent in a digital world where the terms and conditions take an all or nothing approach.

The foregoing shows that regulators are not only "nice to have" but, in truth, they are fundamental elements in the correct application of the law and of relevant underlining principles.

2.3. The example of Ivory Coast

As an additional note and to demonstrate the importance of regulators as an effective part of the application of law, reference can also be made to the Ivory Coast and its data protection internal legal landscape (enacted by means of Law No. 2013-450, of 19 of June).

In Ivory Coast, we are able to find the same general principles and rules as in the aforementioned examples. Be that as it may, this jurisdiction has gone a step further and it is possible to avoid the necessity of compliance with formalities with the national regulator, the "Authorité de Régulation des Télécommunications" ("ARTCI"), with the appointment of a Data Protection Officer.

More to the point, should a person qualifies as a Data Protection Officer, under local regulations[10], the same can act as a sort-of representative of ARTCI within their own entities (or at least as an independent gatekeeper of the values and rules set in the law) and, as such, audit themselves the application of the law without the need to make filings with the regulator. This exemption to comply with formalities is only voided in specific circumstances, such as special operations of processing of data are involved (e.g. sensitive data).

3. Where do we go from here?

Although it seems unquestionable that Africa has been taking important steps in protecting privacy and personal data, the current scenario is still far from ideal.

[10] In order for natural or legal persons to fulfil the role of a Data Protection Officer in Ivory Coast, they must meet certain criteria. Said rules are laid down in Order No. 511/MPTIC/CAB of 11 November 2014, which defines the relevant profile and lays down the relevant employment conditions. Among other conditions, Data Protection Officers must have completed a certain level of studies in legal sciences or computer sciences or Telecommunications/ICT networks and must be Ivorian citizens.

Historically, African countries are not particularly known for taking a unified and cohesive approach between all its States, although there are very successful cases at regional level. In seldom occasions have all African states taken a single stance at international level.

In the case of data protection and on the verge of an increasingly digital world where borders are almost inexistent, Africa cannot be isolated from the rest of the World. Thus, although the legal landscape has already some density, the same will most likely to be revised given the changes that we are seeing in places such as the European Union. By means of example, the new GDPR, which will become effective in May 2018 and will regulate all data protection operations in Europe, presents much stricter rules on issues such as cross-border transfer of data, making it impossible to transfer data for countries that fall short under said standards.

Furthermore, the global paradigm seems to be shifting from a hetero to an auto regulation and, most likely, at a moment, the local regulators will seek to act not as guardians of innumerous fillings but as real “knights” of the law, by means of audits and other continuous activities. This will not only serve the purpose of ensuring that the law is being applied in a correct and contemporaneous way, but also will more actively fight issues such as preventing money laundering, corruption and nepotism.

In other words, while we cannot forget that Africa is a complex reality and its own set of singularities, Africa is not alone for all of us. Regardless of where we stand, we are now in a brave new (digital) world.

Lisbon, 20 July 2017

João Luís Traça

AREAS OF PRACTICE

IP and TMT

EXPERTISE

IP

Data Protection

TMT

EDUCATION AND TRAINING

1999-2001: MBA - Portuguese Catholic University
1995: Admitted to the Portuguese Bar Association
1988-1993: Degree in Law - Portuguese Catholic University

WORK EXPERIENCE

Since 2002: Partner - Miranda
1996-1999: Director - Esoterica, Internet Service Provider
1995-2002: Associate - Santiago Neves & Associados

LANGUAGES

Portuguese, English, French and Spanish

JURISDICTION GROUPS

Portugal, Angola, Mozambique, Guinea-Bissau, Cape Verde, Cameroon, São Tomé and Principe, Congo, DRC, Gabon and Timor-Leste

DATA PROTECTION RELATED PUBLICATIONS

- Traça, João Luís Traça; Embry, Bernardo, "An overview of the legal regime for data protection in Cape Verde" in *International Data Privacy Law*, Oxford Journals, 2011, p. 249-255
- Traça, João Luís Traça; Embry, Bernardo, "The Angolan Data Protection Act: first impressions" in *International Data Privacy Law*, Oxford Journals, 2012, p. 40-45
- Traça, João Luís Traça; Embry, Bernardo, "The Portuguese regulatory regime for Binding Corporate Rules" in *International Data Privacy Law*, Oxford Journals, 2011, p. 249-255
- Traça, João Luís; Correia, Francisca, "Data Protection in Angola" in *African Data Privacy Laws*, Springer International Publishing AG, 2016, p. 349 - 362
- Traça, João Luís; Gaspar, Pedro Marques, "Data Protection in Cape Verde: An Analysis of the State of the Art" in *African Data Privacy Laws*, Springer International Publishing AG, 2016, p. 249 – 258
- Traça, João Luís; Neves, Lídia, "Data Protection in Mozambique: Inception Phase" in *African Data Privacy Laws*, Springer International Publishing AG, 2016, p. 363 – 370

Contributor to DataGuidance and Nymity