24 Online Dispute Resolution for Africa

Mohamed S. Abdel Wahab

1 Introduction

Africa is vast and rich continent. It is the world's second-largest and second most populous continent.[1] With approximately more than 2000 spoken languages and around 800 dialects used throughout Africa,[2] the Continent is experiencing an accelerated economic growth, especially in sub-Saharan low and middle income States. The African expected economic growth rate is at about 5.0% for 2010 and 5.5% in 2011.[3]

Such rich diversity, which spans the African continent, has certainly impacted its legal culture, especially the dispute resolution culture. However, owing to the numerous economic and technological challenges experienced by Africa, the incorporation of ICT in dispute resolution schemes has not yet been fully utilized. In fact, ICT implementation in traditional dispute resolution schemes as well as the creation of new forms of technology based processes is still at its inception in the overwhelming majority of States. To the exclusion of South Africa, Egypt, and Tunisia, which often receive the highest African rankings in the Network Readiness Index (NRI) developed by the World Economic Forum,[4] African states are grappling to build their ICT infrastructure and bridging the digital divide.[5] However, it is worth noting that Africa now holds ten places in the top 100 states

1 Africa hosts 54 independent states following the split of Sudan and the creation of the Republic of South Sudan. Africa is the second largest continent after Asia, which hosts around 44 independent states. The African continent covers 6% of the Earth's total surface area and around 20.4% of the total land mass. Its population is estimated at around 1 billion people and accounts for approximately 14.72% of the world's population.

2 In addition to Arabic, which is an imported language spoken Africa since the Arab conquest of North Africa over 1400 years ago, there are five major language families, these are: (1) *Afro-Asiatic*; (2) *Nilo-Saharan*; (3) *Niger-Kordofanian*; (4) *Khoi-San*; and (5) *Austronesian*. See <http://africanlanguages.com>, last accessed 15 June 2011.

3 IMF; World Economic Outlook, Recovery, Risk, and Rebalancing (2010) p. 88. Data available at <www.imf.org/external/pubs/ft/weo/2010/02/pdf/c2.pdf>, last accessed 15 June 2011.

4 According to the 2011 Global Information Technology Report, Tunisia ranked 35th, South Africa ranked 61st, and Egypt ranked 74th on the 2010-2011 NRI. See World Economic Forum; Global Information Technology Report (2010-2011). Data available at <http://reports.weforum.org/global-information-technology-report/>, last accessed 15 June 2011.

5 The term "digital divide" denotes "the gap between individuals, households, businesses and geographic areas at different socio-economic levels with regard both to their opportunities to access information and communication technologies (ICTs) and to their use of the Internet for a wide variety of activities. The digital divide reflects various differences among and within countries". See OECD; Understanding the Digital Divide (2001) p. 5. Available at <www.oecd.org/pdf/ M00002000/M00002444.pdf>, last accessed 15 June 2011. For

on the NRI, where the Gambia ranks the 76th, Senegal ranks the 80th, Kenya ranks 81st, Namibia ranks 82nd, Morroco ranks 83rd, Botswana ranks 91st, and Ghana ranks 99th.[6]

Owing to the fact that ODR essentially involves utilizing ICT applications to, directly or indirectly, resolve disputes, it is a prerequisite for ODR to have an efficient techno-legal framework that can support ODR modalities.

Information technology, the Internet, wide area networking techniques, and broadband connections have made it possible for anyone to transmit significant amounts of information across the globe instantaneously, which improves the conditions of the global economy, accelerates the growth of e-commerce, and creates an apposite milieu for the development of ODR. Thus, it seems in order to shed light on the ICT *status quo* in Africa to enable readers to comprehend the challenges to ODR implementation in Africa.

That said, this chapter, which aims at analyzing the use of ODR in Africa, shall first provide a succinct analysis of ICT in African countries, as ICT applications constitute the foundational basis and readiness for the use of ODR in Africa (section 2). Subsequently, reference shall be made to the legal and regulatory matrix of laws and regulations adopted in the techno-leading African countries,[7] as such matrix is indispensable for boosting trust and e-confidence in ODR schemes (section 3). Thereafter, a special note of domain names disputes seems in order as such sector specific disputes are already paving the way for the proper implementation of ODR in Africa (section 4). Finally, the chapter shall conclude by providing a pathway for the future of ODR in Africa including specific references to the most appropriate and appealing sectors for ODR services (section 5).

2 Africa's ICT Readiness: Challenges and Requisites to ODR

Africa now comprises of fifty-three fully recognized and independent countries. However, such states differ with respect to their ICT capacity and applications. Several factors contribute to such existing ICT variation amongst African states.

In order to pave the way for diffusion of ODR services and schemes, the development of a solid ICT infrastructure is indispensable. In recent years, specifically since the 2003 Geneva World Summit on the Information Society and the 2005 Tunisia World Summit

a brief survey of some of the international projects and schemes that aim at inducing ICT diffusion and development in LDCs and disadvantaged regions, see M. Wahab, "The Digital Divide, E-Commerce, and ODR: Constructing the Egyptian Information Society", in E. Katsh, D. Choi, A. Gaitenby and C. Rule, *Online Dispute Resolution (ODR):Technology as the "Fourth Party", Papers and Proceedings of the 2003 United Nations Forum on ODR*, p. 9-13. Available at <www.odr.info/unece2003/pdf/wahab.pdf>.

6 See World Economic Forum; Global Information Technology Report (2010-2011). Data available at <http://reports.weforum.org/global-information-technology-report/>, last accessed 15 June 2011.

7 These are currently Tunisia, South Africa, Egypt and Morocco.

on the Information Society,[8] African States began to develop and boost their ICT capabilities. This includes due consideration of several indicators, namely: (1) *Infrastructure indicators* (Personal computers, mainlines and mobiles subscribers, Internet users and 3G Subscribers, broadband usage, number of Internet hosts and security of the Internet servers); (2) *Capacity indicators* (Illiteracy rates, public expenditure on education and International Internet bandwidth); and (3) *Financial indicators* (Gross Domestic Product (GDP), Foreign Direct Investment (FDI) and Public and private investments in telecommunications). Each of these indicators merits a mention herein below.

2.1 Infrastructure Indicators

Generally, most countries in Africa saw an average of 10% increase in the number of people who own a personal computer in 2006-2007, and the percentage is increasing at an accelerated pace. Egypt is, by far, the country with the highest number of people owning computers (over three million in 2007). Conversely, the number of personal computers in Sub-Saharan Africa (excluding South Africa and Nigeria) went down from seven million to just a million between 2006 and 2007. However, the North African region maintains the highest number of people owing PCs amongst African States. This is largely due to Egypt, Tunisia, and Morocco.[9]

The number of fixed lines and mobile phone subscribers has gradually increased between 2006 and 2008. The highest rate of increase has been witnessed by Nigeria, which had around thirty-four million in 2006 and jumped to over fifty-three million in 2008. Egypt ranked second; from around 28million in 2006 to over fifty-three million in 2008. The North African region in general has witnessed the highest growth compared to other regions, although the Sub-Saharan region is experiencing growth but at a slightly lower rate. Central and Southern part of Africa witnessed 200% growth. This includes Ethiopia, Kenya, Madagascar, Tanzania and Uganda.[10] Strikingly, both Mauritius and Seychelles have over 1,000 subscribers per 1,000 inhabitants which suggests that many people are subscribed to more than one fixed line and/or mobile phone line.[11]

More specifically, from 2006 to 20008, the number of mobile phone subscribers had significantly increased. Whilst both Kenya and Egypt had much more subscribers, Ethiopia had fewer than one million in 2006 and three million in 2008. The Sub Saharan region saw large increases, basically double the amount of subscribers in 2008 comparing to 2006.[12]

---

8 See <www.itu.int/wsis/index.html>, last accessed 15 June 2011.

9 World Bank; Africa Development Indicators (March 2010); data available at <http://databank.worldbank.org/ddp/home.do?Step=12&id=4&CNO=1147>, last accessed 15 June 2011.

10 *Id.*

11 *Id.*

12 *Id.*

There has also been notable growth in some African countries with respect to subscription to 3G applications and services. In 2009, some countries witnessed annual growth of more than 100%. For example, Libya had over 300% growth, Morocco had more than 200%, and South Africa had more than 100%. Egypt only witnessed 83% growth. It is worth highlighting that Tanzania experienced a notable decrease by 22%.[13]

With respect to Internet users, there has been an increase of nearly fifteen million people between 2006 and 2008. Egypt, Morocco, and Nigeria had the highest number of Internet users. The Sub-Saharan developing region had over thirty-five million users in 2008, which means that despite having relatively low number of personally owned PCs, people, in this region, still had adequate access to the Internet. The North African region ranked second with respect to the highest penetration of Internet users, largely due to both Egypt and Morocco.[14]

With respect to broadband access, some countries have witnessed exponential growth such as Mauritius, Mauritania, Egypt, and Tunisia, which had large increases in broadband subscribers between 2006 and 2008.[15] On the other hand, the Sub-Saharan developing region experienced a decrease in this context.[16] The North African region witnessed an increase to nearly 1.5 million in 2008 compared to only 0.8 million in 2006.[17]

Between 2006 and 2008, International Internet bandwidth (bits per person) has increased in Egypt, Cape Verde, and Mauritius. Tunisia, Sudan, Morocco and Seychelles, where they have witnessed massive increase from as little as five bits per person to well over 1,000 bits per person.[18]

With respect to the number of Internet hosts across African countries, this largely differs. Generally, the North African region has developed a high number of Internet hosts in 2010, with mainly Egypt containing over 187,000 hosts and Morocco having over 277,000 hosts.[19] Surprisingly, Tunisia had only 490 hosts in 2010.[20] It is worth mentioning that whilst Egypt has a higher number of PC owners than Morocco, the latter has more Internet hosts. It is also worth noting that whilst Ghana has over 41,000 Internet hosts, Nigeria only had 1,300 hosts in 2010, despite the fact that the latter State has a high Internet penetration rate.[21] Nonetheless, South Africa has, by far, the highest number of Internet hosts throughout the whole of Africa, with over three million servers, despite the fact that South

13 *Id.*
14 *Id.*
15 *Id.*
16 *Id.*
17 *Id.*
18 *Id.*
19 Central Intelligence Agency; The World Fact book (2010); data available at <https://www.cia.gov/library/publications/the-world-factbook/rankorder/2184rank.html>, last accessed 15 June 2011.
20 *Id.*
21 *Id.*

Africa, when compared to Egypt and Morocco, had lower Internet penetration rates with only over four million.[22]

With respect to secure Internet servers, which are indispensable for secure e-commerce and ODR applications, the security thereof has been gaining due attention in the majority of African States since 2006. Whilst South Africa hosts the highest number of secure servers, both Nigeria and Tunisia have over 100 secure servers. Egypt, although having the highest number of owned PCs and very high Internet penetration rate as previously mentioned, is still providing fewer secure servers when compared to Tunisia or Nigeria.[23]

2.2 Capacity Indicators

Given the fact that most African states are developing nations, this certainly impacts education and illiteracy rates, which seem to be quite high in some African countries. Despite the high number of Internet users in Egypt, the basic illiteracy rate is 34% of people aged fifteen years and above.[24] Morocco suffers from 44% illiteracy rate.[25] Senegal equally has a high illiteracy rate of 58%, despite the colossal increase in Internet users between 2006 and 2008.[26] The highest illiteracy rates tend to exist in Chad (68%), Burkina Faso and Niger (71%), and Mali with the highest rate in Africa (74%).[27] On the other hand, Zimbabwe has the lowest rate (9%).[28] In all African countries, it seems evident that females are suffering from more illiteracy than males, which makes it interesting to assess the correlation between gender illiteracy and gender Internet usage in these countries.[29]

The percentage of public expenditure on education in general seems low, with Lesotho having the highest (12.4%) and Chad being one of the lowest (1.9%).[30] Both Egypt and Morocco have spent as low as (3.7%) and (5.5%), respectively. Conversely, in the Southern African region, some countries tend to have high expenditure rate such as Botswana (8.1%) and Swaziland (8.3%) even though both experience relatively low Internet usage as well as low Foreign Direct Investment (FDI). In the Northern region, Tunisia seemed to have

22 *Id.*
23 World Bank; Africa Development Indicators (March 2010); data available at <databank.worldbank.org/ddp/home.do?Step=12&id=4&CNO=1147>, last accessed 15 June 2011.
24 Organization for Economic Co-operation and Development; African Economic Outlook; Data & Statistics; Table 18, Basic Education Indicators, Excel spreadsheet (2011); available at <http://www.africaneconomicoutlook.org/en/data-statistics/>, last accessed 9 June 2011.
25 *Id.*
26 *Id.*
27 *Id.*
28 *Id.*.
29 *Id.*.
30 *Id.*.

spent slightly more than Egypt and Morocco, and this is indeed reflected in the lower levels of illiteracy.[31]

2.3 *Financial Indicators*

According to the latest verified statistical information, the period between 2006 and 2009 shows that the average growth rate of real GDP in Africa is 5% per year except for 2009 where the growth rate was lower than usual owing to the global financial crisis that swept the world in 2008.[32]

Generally, in both 2006 and 2007, 6% of GDP in the whole of Africa was spent on ICT. It is interesting to note that the North African region had spent 5% of their GDP, mainly due to Algeria, Egypt, Tunisia and Morocco. South Africa and Senegal spent 10% and 11%, respectively.[33] The figures provided for 2006 were exactly the same for 2007. Thus, there were no deviations in expenditure in both years.[34]

With respect to FDI, it has witnessed fundamental changes between 2006 and 2009. Whilst some countries have benefited from an increase, others have suffered from a decrease in FDI. Angola had the highest FDI, with 13,101 million USD in 2009.[35] In addition, Algeria, Ghana, Niger and Equatorial Guinea witnessed a strong increase in FDI.[36] On the other hand, Kenya exhibited a mixture of both an increase and decrease between 2006 and 2009, where it was 51 million USD in 2006, 729 million USD in 2007, 96 million USD in 2008, and 141 million in 2009.[37] In 2009, Morocco witnessed a decrease of FDI outflows compared to 2007, dropping from 621 million USD in 2007 to 470 million USD in 2009. Moreover, their FDI inflows in 2009 decreased by almost half from 2487 million USD in

31 *Id.*

32 Organization for Economic Co-operation and Development; African Economic Outlook; Data & Statistics (2011); data available at <www.africaneconomicoutlook.org/en/data-statistics/table-2-real-gdp-growth-rates-2001-2011/>, last accessed 15 June 2011.

33 World Bank; Africa Development Indicators (March 2011); data available at <databank.worldbank.org/ddp/home.do?Step=12&id=4&CNO=1147>, last accessed 15 June 2011.

34 *Id.*

35 Organization for Economic Co-operation and Development; African Economic Outlook; Data & Statistics (2011); data available at <www.africaneconomicoutlook.org/en/data-statistics/table-10-foreign-direct-investment-2003-2008-usd-million/>, last accessed 9 June 2011.

36 Organization for Economic Co-operation and Development; African Economic Outlook; Data & Statistics (2011). From 2006 to 2009, FDI increased from 1795 million USD to 2847 million in Algeria, 636 to 1685 million USD in Ghana, 470 to 1636 million USD in Equatorial Guinea and 51 to 739 million USD in Niger. Data available at <www.africaneconomicoutlook.org/en/data-statistics/table-10-foreign-direct-investment-2003-2008-usd-million/>, last accessed 9 June 2011.

37 Organization for Economic Co-operation and Development; African Economic Outlook; Data & Statistics (2011); data available at <www.africaneconomicoutlook.org/en/data-statistics/table-10-foreign-direct-investment-2003-2008-usd-million/>, last accessed 9 June 2011.

2008 to 1331 million USD in 2009.[38] Libya had the highest outflow of investments of 5888 million USD in 2008 but sharply decreased to 1165 million USD in 2009.[39] Egypt's outflow of FDI increased from 148 million USD in 2006 to 1920 million USD in 2008, but decreased to 571 million USD in 2009, which equally occurred with respect to Egypt's FDI inflows that decreased from 9495 in 2008 to 6712 in 2009.[40] South Africa had a negative outflow of FDI of 3533 million USD in 2008 which increased in 2009 to 1584 million USD and an important increase of 9009 million USD in 2008 of FDI inflows compared to 5695 million USD in the previous year, followed by an important decrease in 2009 with an FDI inflow of 5696 million USD.[41]

In the context of ICT, investments in telecommunications with private participation in most African countries generally decreased between 2006 and 2007. However, in Cameroon, Ghana, Senegal, and Liberia investments increased by a high proportion.[42] North Africa, witnessed a decrease in ICT investments, and specifically in Tunisia there was a dramatic drop.[43] However the Sub-Saharan region witnessed some important increase in investments, especially in the Niger, Chad, Swaziland, and Malawi.[44]

In light of the above succinct overview of the diverse indicators and factors that determine African States' ICT readiness, it seems plausible to distinguish between three different groups of African States: (1) ICT ready States such as South Africa, Egypt, Morocco and Tunisia; (2) ICT progressing States such as Nigeria, Cameroon, Tanzania, Algeria, Seychelles, and Ghana and (3) ICT potentially progressing States such as Botswana, Malawi, Zambia, Central Africa, Chad, Niger, Guinea, Somalia, Ethiopia, Burkina Faso, Sierra Leone, Ivory Coast, Burundi, and Rwanda.

---

38 *Id.*

39 *Id.*

40 *Id.*

41 Organization for Economic Co-operation and Development; African Economic Outlook; Data & Statistics (2011); data available at <www.africaneconomicoutlook.org/en/data-statistics/table-10-foreign-direct-investment-2003-2008-usd-million/>, last accessed 15 June 2011.

42 World Bank; Africa Development Indicators (March 2011). From 2006 to 2007, investment in telecoms with private participation increased in Cameroon from 63 million USD to more than 149 million USD, in Ghana from 215 million to 420 million USD, in Senegal from 212 million to 567 million USD and in Liberia from more than 10 million USD to 17 million USD. Data Available at <http://databank.worldbank.org/ddp/home.do?Step=12&id=4&CNO=1147>, last accessed 15 June 2011.

43 World Bank; Africa Development Indicators (March 2011). From 2006 to 2007, Tunisia witnessed a drop of investment in telecoms with private participation from 2343 million USD to 76 million USD. Data Available at <http://databank.worldbank.org/ddp/home.do?Step=12&id=4&CNO=1147>, last accessed 15 June 2011.

44 World Bank; Africa Development Indicators (March 2011). From 2006 to 2007, investment in telecoms with private participation increased in Niger from 0 to 110 million USD, in Chad from more than 26 million USD to more than 53 million USD, in Swaziland from 0 to almost 4 million USD and in Malawi from more than 30 million to 37 million USD. Data available at <http://databank.worldbank.org/ddp/home.do?Step=12&id=4&CNO=1147>, last accessed 15 June 2011.

It is also manifest that the proliferation of ODR in Africa is decelerated by the scarcity of adequate ICT infrastructure and capacity indicators. This seems to be changing in light of the relative increase in financial indicators, especially FDI and ICT expenditure. Nevertheless, enhancing ICT infrastructure and developing capacity to offer state-of-the-art ODR services hinge not only on ICT, capacity, and financial readiness, but also on the existence of adequate socio-legal infrastructure that provides compatible regulatory framework that boosts trust and confidence. This would ultimately create cultural readiness for ODR in Africa.

On such account, it seems necessary to provide a brief overview of ODR related legal and regulatory frameworks in some of the ICT ready and progressing African States, which will eventually support fully-fledged ODR schemes.

3 ICT Laws and Regulations: Boosting E-Trust and E-Confidence

The indispensability of adequate socio-legal and regulatory framework for ODR has been emphasized by UNCTAD, which stated:

> The need for an appropriate legal framework that is supportive of and conducive to the practice of e-commerce has been identified as a prerequisite for the growth of e-commerce in general and ODR in particular.[45]

At the outset, the majority of African and Middle Eastern States are predominantly legislation centric. In other words, the prevailing legal culture in such regions is founded on statutory instruments, which serves a dual purpose, that is: (a) regulating specific sectors, services, and/or activities; and (b) boosting public trust and confidence in such regulated services and activities. That said, the proliferation of ICT applications and services, especially ODR schemes, require the existence of a solid matrix of supporting laws and regulations.[46]

On such account, Africa generally lacks sufficient ICT and ODR oriented legislative instruments, including, but not limited to, the full recognition of electronic data messages and communications, e-commerce, and/or data protection. Nevertheless, some ICT ready and progressing African States, such as Egypt, Tunisia, Morocco, Algeria, and South Africa,

45 UNCTAD; "E-Commerce and Development Report 2003" (2003); Chapter 7: "Online Dispute Resolution: E-Commerce and Beyond." data available at <www.unctad.org/en/docs/ecdr2003_en.pdf>, last accessed 15 June 2011.

46 It is worth noting that other regions and countries may principally rely on market practices irrespective of any statutory instruments. This is generally accepted in advanced and highly developed states, where the State generally opts for a non-interventionist approach, due to powerful market forces that efficiently contribute to the development and shaping of the relevant norms and practices.

have witnessed, over the past few years, a proliferation of several legislative initiatives that support ICT applications and services.

Prior to embarking on a brief survey of such initiatives, it seems in order to identify the pertinent key legislative instruments that support ICT. These include (A) E-commerce, E-contracting, and Digital Signature, (B) E-evidence (admissibility and evidentiary weight), and (C) Protective Laws (Intellectual Property Rights, Consumer Protection, and Information and Cyber-security regulation).

3.1 E-Commerce & Digital Signature Laws

E-commerce allows consumers and businesses to conduct business through electronic means on national, regional, and global levels. Whilst most advanced African countries have adequate e-commerce norms in place, less developed regions and states are increasingly recognizing the importance of an e-commerce legal framework.

In Egypt, the accelerated growth in Internet usage and utilization has prompted the development of B2B and B2C e-commerce and regulation,[47] which has resulted in the enactment of the Digital Signatures Law No. 15 of 2004 (E-Sign Law) and the establishment of the Information Technology Industry Development Agency (ITIDA) in 2004.[48] ITIDA supports the development of ICT in Egypt through the following interdisciplinary initiatives: (i) *Research and Innovation Support*, which aims at supporting the development of mature innovation management systems in Egyptian ICT SMEs that would enable such entities to introduce competitive innovative ICT products and services into the marketplace; leading to a considerable boost to Egypt's national GDP; (ii) *Small and Medium Enterprises*, which are important to the growth of Egypt's ICT sector. Owing to Egypt's tax, custom and financial sector reforms, it has acquired a strong position to provide outstanding incubation management to seed and startup IT companies and boost employment skills through training schemes; (iii) *Enterprise International Certification* through participating in a number of international certification programs to achieve recognition and certification of Egyptian companies and improve their skill base; (iv) *Information Technology Academia Collaboration* (ITAC), which aims at promoting and incentivizing research projects that bring value to IT companies, universities, research centers and the wider technological community in Egypt, and has been designed to link industry research with market needs;

47 B2C e-commerce sites in Egypt include stock market trading, real property, food delivery, lifestyle products, Egyptian handicrafts, furniture and human-resources industries.

48 ITIDA is the executive IT arm of the Egyptian Ministry of Communications and Information Technology, MCIT. With local and international outreach, ITIDA plays a fundamental role as a one-stop-shop for foreign direct investors seeking to enhance their global offering using Egypt's competitive advantages. ITIDA actively pursues two broad goals: (i) building the capacities of Egypt's ICT sector, and (ii) attracting FDI to boost the ICT sector locally and globally. See <www.itida.gov.eg>, last accessed 9 June 2011.

(v) *Industry Development* through supporting local Egyptian businesses and increasing their international exports; and (vi) *Community Awareness* through prioritizing the development of the software industry whilst increasing social awareness of intellectual property issues. As a result of these programs, Egypt's piracy rating has dropped from 69% in 2003 to 59% in 2009 according to the seventh annual BSA and IDC Global Software Piracy Study.[49]

With respect to E-signature services for the public and private sectors, such services were launched on 28 September 2009 together with the inauguration of the Egyptian Root-CA trust center, marking the e-signature authorization system by the ITIDA. ITIDA, as a supervisory body for electronic signature, operates the Egyptian Root Certificate Authority (Root CA) and the E-signature CA Licensing Unit. The Root CA will issue digital certificates to subordinate Certificate Service Providers (CSP) to provide the proper infrastructure for the use of E-signature in Egypt. The Egyptian E-signature CA Licensing Unit has been set up to audit the E-signature service providers companies in Egypt, address complaints, offer technical counseling in collaboration with the Root CA panel, and mediate between disputing parties, forming part of the ICT Industry ombudsman within ITIDA framework. A limited number of Egyptian E-signature Service Providers (ESPs) have been licensed by the E-signature CA Licensing Unit, in order to provide e-signature services, issue digital certificates and corresponding electronic signatures for citizens and private sector companies' clients.[50]

With respect to IPR, the new IPR Law No. 82 of 2002 unifies and supersedes existing intellectual property laws, some of which date back over half a century. It is designed to bring Egypt's legislation into compliance with the Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement. The Law covers copyrights, models and industrial designs, patents of invention, utility models, layout designs of integrated circuits, undisclosed information, and trademarks.[51] This Law has contributed to the creation of an environment that encourages creativity and boosts FDI.

---

49 See <www.itida.gov.eg/En/OurPrograms/Pages/default.aspx>, last accessed 9 June 2011.

50 To-date, there are four licensed companies: Security & Network Services ("SNS"), Misr for Central Clearing, Depository and Registry ("MCDR"), Egypt Trust, and Advanced Computer Technology ("ACT"). The list of licensed companies and their contact information is available at <www.egypton.com/En/Ourprograms/IndustryInfrastructure/eSignature/Pages/default.aspx>, last accessed 9 June 2011.

51 Although Law No. 82 of 2002 expands the scope of protection so as to include items that have not been protected before such as utility models, topographies of integrated circuits and undisclosed information, yet it does not provide an explicit reference to the protection of ICT applications in the context of IPR except in the context of copyright protection. For example, explicit reference was made in Article (138) to the audio or audio-visual transmission of work, performance, phonogram or the work or performance recording, to the public by wireless means including satellite broadcasting. Moreover, Article (140) states that rights of the authors to their literary and artistic works shall be protected by the law herein, and particularly computer software and databases which are either legible by computer or by any other device. Furthermore, Article (181) provides for penalties by imprisonment for not less than one month and/or a fine of not less than 5,000 Egyptian pounds, and not exceeding 10,000 Egyptian pounds, for publishing a work, phonogram,

Moreover, Egypt has enacted the Telecommunication Law No. 10 of 2003. This Law aims at reorganizing the telecommunications sector, and is based on some fundamental principles, amongst which are: universal access, party autonomy, protection of users, and encouraging investment in the ICT sector. The Law established the National Telecommunications Regulatory Authority (NTRA), which is entrusted with the organization of the telecommunications utility and issuing telecommunications licenses in accordance with the above-mentioned fundamental principles. The Law also provides for severe penalties of imprisonment for a period not less than three months and/or a fine not less than L.E 5,000 and not exceeding L.E. 5,0000 for the publishing, recording, hiding, obstructing, modifying, and/or refraining from sending the contents of a communications message or part of it without having any legal basis for such action. The same penalties apply for divulging information concerning users of communication networks and their communication.[52]

In Morocco, the Moroccan Law No. 53-05 for electronic exchange of legal data was enacted in 30 November 2007.[53] The Law governs the electronic signature legal framework in Morocco and regulates electronic certification and cryptography. The Law modifies and complements Articles (417), (425), (426), (440), and (443) of the Moroccan Civil Code and was adopted a month after the decision of the Professional Group of Moroccan Bank (*Groupement Professionnel des Banques Marocaines*) allowing online payment with Moroccan credit cards.[54]

According to Article (6) of the Moroccan Law, a secure electronic signature is produced by a device for creating electronic signatures attested by a certificate of compliance issued by the National Telecommunications Regulatory Agency (ANRT), designated as the National Authority for Approval and Monitoring of Electronic Certification. Its role is therefore to accredit providers of electronic certification.

The Executive Regulations of the Law were enacted two years later and specifically on 18 June 2009.[55] The Regulations addressed means of encrypting data messages and condi-

---

broadcast or performance protected pursuant to the provisions of the law herein via computers, Internet, information networks, communication networks or any other means, without having prior written permission from the author or holder of the neighbouring right.

52 See Article (73) of the Telecommunications Law.

53 *Loi No. 53-05 relative à l'échange électronique de données juridiques*. Available at <http://droitmaroc.wordpress.com/2008/01/29/loi-n%C2%B0-53-05-relative-a-lechange-electronique-de-donnees-juridiques-integrale/>, last accessed 15 June 2011.

54 *Commerce électronique au Maroc* (E-Commerce in Morocco), Online publication, July 2010. Available at <http://ennasri.centerblog.net/5-commerce-electronique-au-maroc>, last accessed 15 June 2011.

55 *Décret n° 2-08-518 du 25 joumada I 1430 pris pour l'application des articles 13, 14, 15, 21 et 23 de la loi n° 53-05 relative à l'échange électronique des données juridiques* (Decree No.2-08-518 of 25 JoumadaI 1430 executing Articles 13, 14, 15, 21 and 23 of Law No. 53-05 for electronic exchange of legal data); Official Bulletin No. 5744; 18 June 2009. Available at <www.cabinetbassamat.com/fileadmin/Codes%20et%20lois/Droit%20de%20l’immatériel/decret%20echange%20electronique%20des%20donnees%20juridiques.pdf>, last accessed 15 June 2011.

tions for electronic certification of providers requesting accreditation. Nevertheless, hitherto, no provider has been accredited. Only some public agencies, through their internal certification process, provide electronic signature services. For example, the Moroccan National Social Security Fund (CNSS) has its own certification authority and thus offers employers the opportunity to report and pay payroll taxes over the Internet through its website damancom.ma. In essence, e-government services have preceded e-commerce and B2B transactions in Morocco.[56]

In Tunisia, the Electronic Exchange and Electronic Commerce Law was enacted since 9 August 2000.[57] This Law, which is certainly inspired by the French Law No. 2000-230 of 13 March 2000, deals with electronic signatures and affords e-signatures and e-documents the same evidentiary weight afforded to paper-based documents in so far as the authenticity conditions are fulfilled. In Tunisia, the electronic signatures system uses the public key infrastructure (PKI) system/encryption, which is the same technology utilized under the Egyptian E-Sign Law.[58]

The Executive Regulations of the Tunisian Law have been adopted in 2001 by virtue of the Decree No. 2001-1667 of 17 July 2001, which establishes specifications for undertaking the activity of electronic certification services provider. Moreover, Decree No. 2001-1668 of 2001 has laid down the procedure for obtaining permission to carry out the activity of electronic certification services provider, and Decree No. 2001-2727 of 20 November 2001 sets the conditions and procedures to use cryptography and encryption. Furthermore, two internal order (*Arrêtés*) of the Tunisian Ministry of Communication and Technologies of 19 July 2001 have determined the technical specifications for digital certificates, their reliability and technical characteristics of the device creating electronic signatures.

In Algeria, a legislative amendment of Articles (323 *bis*), (323 *bis* 1) and (327) of Algerian Civil Code has been passed in April 2005, allowing the use of electronic evidence. However, Algeria has not yet adopted a separate and specific legislation on electronic signatures. Two draft laws should have been finalized by the first part of 2010, but no indication has been found showing that those drafts have now been enacted.[59] The first of these draft laws aims at regulating electronic exchanges and includes provisions relating to

56 It is also worth noting that Egypt offers a number of e-government services to citizens, businesses, and foreigners through its government portal. See <www.egypt.gov.eg/english/>, last accessed 9 June 2011.

57 *Loi No. 2000-83 du 9 août 2000, relative aux échanges et au commerce éléctronique* (Electronic Exchange and Electronic Commerce Law), 9 August 2000. Available at <www.certification.tn/fileadmin/Documents/loi_2000-83_fr.pdf>, last accessed 15 June 2011.

58 It is worth noting that both Egyptian and Tunisian Laws are not technology neutral but have specifically opted for a PKI system to the exclusion of new technologies such biometrics. This is quite questionable, especially that technology specific laws are generally undesirable owing to the fact that technological applications become antediluvian within a relatively short time span.

59 Anonymous Author, "Algérie: Un projet de loi pour sécuriser Internet (Algeria: draft law to secure Internet)", *Le quotidien d'Oran* (Oran Daily Newspaper), Online Publication, 10 May 2010. Available at <www.city-dz.com/algerie-un-projet-de-loi-pour-securiser-internet/>, last accessed 15 June 2011.

electronic certificates, electronic signature and cryptography. The second one is related to the protection of personal data and aims at maintaining a strict framework for the protection of Internet users.

On a different note, leaving the North African region to South Africa, it seems evident that e-commerce in increasingly utilized in South-Africa. The Telecommunications Act No. 103 of 1996 has generated a matrix of legislative instruments. The 1996 Act was amended by the Telecommunications Amendment Act No. 12 of 1997, the Independent Communications Authority of South Africa Act No.13 of 2000, and the Telecommunications Amendment Act No. 64 of 2001. In July 2001, the Independent Communications Authority of South Africa (ICASA) was established and merged both the Telecoms Regulator (Telecommunications Regulators Association of Southern Africa) and the Broadcasting Regulator (Independent Broadcasting Authority).

In July 2006, the Electronic Communications Act (ECT) was promulgated in 2002 to regulate and promote electronic communications and transactions, consumer protection, e-government services and e-signatures.[60]

3.2 E-Evidence Regime

Owing to the fact that diverse ODR schemes involve electronic exchange of documents, which may very well be intrinsically electronic in nature and format, the validity and evidentiary weight of e-documents become indispensable. Accordingly, e-evidence denotes the legal value and admissibility of electronic, and electronically exchanged, data.

In technology ready African States, it is incontrovertible that e-documents and e-data are admissible as e-evidence, and are afforded the same evidentiary weight as standard paper based documents. In Egypt, Articles (14) and (15) of the E-Sign Law states that e-signatures and e-documents shall have the same determinative and evidentiary effect that standard paper based signatures, writing, official and unofficial communications have under the Code of Evidence. Moreover, Article (16) of the E-Sign Law states:

> The hardcopy of an official electronic document shall have the same determinative effect vis-à-vis all parties and third parties to the extent that this hardcopy conforms to the original official electronic document and in so far as the official electronic document and the e-signature exist on an electronic instrument or medium.

60 Electronic Communications and Transactions Act, No. 25 of 2002. Available at <www.internet.org.za/ect_act.html>, last accessed 15 June 2011.

Such provision is certainly invaluable as it affords reproduced paper-based documents the same evidentiary weight of an electronic original in so far as the electronic original is stored on an e-medium or instrument.[61]

In Morocco, the above mentioned Moroccan Law No. 53-05 for electronic exchange of legal data of 30 November 2007 and its corresponding decree No. 2-08-518 of 6 May 2009 afford legal recognition to data messages and electronic signatures and confirm the full evidentiary weight of e-documents, signatures, and communications in so far as such electronic formats are technologically compliant to ensure their authenticity, ability to unveil any alteration or change, and undoubted attributablity to their author.[62] Moreover, Article (417-1) of the Moroccan Civil Code, introduced by Moroccan Law No. 53-05 states:

> An electronic document has the same force of a written paper-based document. An electronic document shall be allowed as evidence in the same manner as a written paper-based document, provided that the person that issued it can be properly identified and that the electronic document is reliable.[63]

Furthermore, the Moroccan Press Code, in its new version of 2002, imposes restrictions on publishing information criticizing the monarchy, Islam and the country's integrity, and, more specifically, the Sahara dispute. Article (38) of the Press Code lists all electronic means of disseminating information on the above-mentioned issues, including the Internet. This clearly constitutes an implicit, if not explicit, recognition of the legal value and evidentiary weight of electronic data.

In Tunisia, the Tunisian Law on Electronic Exchange and Electronic Commerce No. 2000-83 of 9 August 2000 recognizes e-documents and e-signatures as previously mentioned. It affords the full legal value and weight to electronic signatures and documents.

In South Africa, the enactment of the Computer Evidence Act in 1983, marked a new era in the admissibility of computer print-out in civil cases if certain technical conditions are fulfilled, which clearly demonstrates South Africa's leading role in ICT applications. However, the practical problems experienced in the implementation of the Computer Evidence Act led the South African Law Commission to recommend abolishing the said

61 The importance of such principle is evident in the context of all ODR schemes where any printing or reproduction of e-documents (such as e-awards, e-decisions, e-settlements, and e-contracts, and/or e-communications) in paper format would not, automatically, reduce the evidentiary weight of such paper-based document(s), which are simply a reproduction of the original e-document.

62 Anonymous Author, *La signature électronique vaut preuve juridique mais les certificateurs manquent à l'appel* (Great legal value of electronic signature but certificate Authorities are missing), Online publication, 15 April 2010. Available at <www.maroc-biz.com/data_5/even_detail.php?id=193>, last accessed 15 June 2011.

63 See, for example, the Moroccan Supreme Court Judgment No. 730 of 27 June 2007, which considered the fax as "a valid mean to prove that the other party has been advised of the shipment or receipt of the goods if the receipt of the fax is established before the Tribuna". Available at <http://68.168.119.106:8080/CabBassamat/upload/juris/ar/001425.pdf>, last accessed 15 June 2011.

law. Nevertheless, despite the recommendations of the Law Commission no new legislation on e-evidence was enacted until 2002, when the ECT was promulgated. Section (15) of the ECT, inspired by Article (9) of the UNCITRAL Model Law on Electronic Commerce, deals with the law of evidence. The ECT referred to "data messages" rather than electronic information or computer information. Section (15) of ECT provides for the general admissibility of data messages if satisfying the ordinary requirements of South African Law of evidence for the admissibility of documents, these are: authenticity; and ability to be produced and presented in their original form. Once evidence is admitted, the court enjoys discretionary powers to decide on the evidentiary weight afforded thereto.

In South Africa, the ECT creates two statutory presumptions in favor of the correctness of data messages, these are: a presumption in favor of the accuracy of business records;[64] and a presumption in favor of advanced electronic signatures.[65]

3.3 Protecting Internet Users

Protection of Internet users or "netizens" is a requisite for the proliferation of e-commerce and the progressive use of ODR. Most advanced African States have enacted specific laws such IPR laws. For example, in Egypt, the IPR Law No. 82 of 2002 replaced a collection of laws dating back to 1939 with a comprehensive and consolidated IPR Code in an attempt to create a milieu of creativity and incentivizing FDI.[66] The four books of the new IPR Code regulate patents, integrated circuit designs, undisclosed information, trademarks, geographical indications, trade statements, industrial designs, copyright and related rights, and plant variety protection. The IPR Code attempts to mirror the provisions of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). However, the Law does not cover personal data protection and information security, which have been drafted in a separate bill, which awaits parliamentary review. Moreover, Egypt has already enacted the Consumer Protection Law No. 67 of 2006, which was promulgated and published on the 20 May 2006.

In Morocco, a corpus of diverse laws exists to regulate IPR. Law No. 17-97 of 15 February 2000 aims at protection of Industrial Property,[67] Law No. 09-08 adopted on

64 Section 15(4) of the ECT.

65 Section 13 of the ECT.

66 Law No. 82 of 2002 Pertaining to the Protection of Intellectual Property Rights, Copyrights and Neighbouring Rights. Available at <www.wipo.int/wipolex/en/text.jsp?file_id=190159>, last accessed 15 June 2011.

67 *Loi No. 17-97 relative à la protection de la propriété industrielle* (Law No. 17-97 related to Industrial property protection), 15 February 2000. Available at <www.enset-media.ac.ma/cpa/Fixe/Loi%20propr%20indust.pdf> (in French), last accessed 15 June 2011.

21 May 2009 regulates personal data protection,[68] and Law No. 08-31 enacted in 2008 provides for consumer protection.

Tunisia has adopted a comprehensive legislation governing IPR, that is the IPR Act adopted in 1994.[69]

Concerning data protection, Tunisia has also enacted Law No. 2004-63 of 27 July 2004 regulates the processing of personal data by requiring prior authorization for processing, consent of the data subject, as well as other standard regulatory provisions governing the accuracy and purpose of such processing as well as liability issues.

Moreover, a Computer Security Act No. 2004-5 was adopted in Tunisia on 3 February 2004 to complete the ICT regulatory matrix. The Law creates cyber-safety measures,[70] and establishes a National Agency of Computer Security to control security of information systems and networks of different public and private organizations.

In South Africa, Intellectual Property Laws cover areas as domain names, traditional knowledge, transfer of technology, patents/copyrights and Trade Marks. The following is a list of some of the Intellectual Property Laws in South Africa: Intellectual Property Rights from Publicly Financed Research and Development Act No. 51 of 2008, Geographical Indications Act No. 32 of 2008, the Trade Marks Act of 1993 as amended in 1997 and 2001, Broadcasting Act No. 4 of 1999, and the Industrial Property Laws Amendment Act of 1997.

Concerning electronic data, the ECT provides principles to be adhered to by subscribers with respect to personal information obtained through electronic means. Similarly to dispositions provided under the Tunisian Law on Data Protection, these principles include: (a) obtaining the express written permission of the data subject for the collection, collation, processing or disclosure of any personal information; (b) only collecting that information necessary for the lawful purposes of the data controller; (c) keeping a record for a period of at least one year after collection of the information of what the information was and the specific purpose for which it was collected; and (d) not disclosing personal information

---

68 *Loi No. 09-08 relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel* (Law No. 09-08 related to personal data protection), 18 June 2009, Official Bulletin No. 5744. Available at <http://droitmarocain.blogspot.com/2009/08/la-loi-n-09-08-relative-la-protection.html> (in French), last accessed 15 June 2011.

69 Tunisia has also enacted more than 25 laws, decrees, and orders governing a myriad of IPR related matters including copyrights (Law No. 2009-33 of 23 June 2009 Amending and Supplementing Law No. 94 36 of 24 February 1994 on Literary and Artistic Property), geographical indications (Law No. 2007-68 of 27 December 2007 on Appellations of Origin, Geographical Indications and Indications of Source for Handicrafts), models and industrial designs (Law No. 2001-21 of February 6 2001 on the Protection of Industrial Designs), patents (Law No. 2000-84 of August 24 2000, on Patents), and trademarks (Law No. 2007-50 of 23 July 2007 Amending and Supplementing Law No. 2006-36 of 17 April 2001 on the Protection of Trademarks and Service Marks).

70 An example of those measures is the "Technical Vulnerability Assessment" which is a form of ethical hacking that aims at unveiling system vulnerabilities, to alert the concerned entity in an attempt to prevent exploitation by hackers and attackers.

to a third party by the data controller unless such disclosure is required or permitted by law or is authorized by the data subject.[71]

Moreover, on 24 October 2010, the Consumer Protection Act (CPA) was passed. The Act also governs electronic transactions. The CPA has been drafted in a manner that averts overriding the provisions of the ECT, and in many instances, it specifically refers to the ECT. In the event of a conflict between the CPA and the ECT, the CPA provides that if circumstances dictate that the provisions of the CPA and the Act cannot be applied jointly, the provision that extends the greater protection to a consumer would ultimately prevail.

In light of the above mentioned, it is evident that both Tunisia and South Africa possess the most advanced ICT regulatory matrix, which ultimately paved the way for the first ODR initiatives in Africa, namely, South Africa's *ZA Dispute Resolution Regulations* (ZADRR) and *OnlineOmbud*.

4 ODR Initiatives in Africa

Despite being a developing continent with sufficient barriers to ICT progression and ODR proliferation, Africa managed to spawn a unique dispute resolution culture with a deeply rooted arbitration oriented processes.

Noting that the introduction of ICTs to dispute resolution processes may take a number of forms varying from importing technology as a mere aiding tool to maximum fusion in the sense that IT applications are in effect employed as ODR schemes, it remains necessary to shed light on Africa's few ODR initiatives, which are primarily in the context of domain names disputes and consumer disputes. Territorially, both are located in South Africa, which has pioneered in catering for the Continent's first initiatives that may well qualify as ODR processes.

4.1 South Africa's Domain Name Dispute Resolution Regulations

Domain name disputes are generally associated with cybersquatting, which involves the pre-emptive registration of trademarks by third parties as domain names. Cybersquatters exploit the first-come, first-served nature of the domain name registration system to register names of trademarks, famous people or businesses with which they are not connected.[72]

71 This regulatory framework is expected to be further enhanced and developed by virtue of a Protection of Personal Information Act, published as a Bill on 14 August 2009, which remains to be enacted. The Protection of Personal Information Act is expected to be applicable to both the private and public sectors and will regulate the manner in which those sectors process personal information.

72 Cybersquatting refers to the *mala fide* registration of a domain name containing another person's brand or trademark in a domain name. Cybersquatting takes two main forms. First, there is "typosquatting" which is the registration of domain names containing variants of popular trademarks. Typosquatters rely on the

Subsequently, cybersquatters often put their domain names up for auction, or offer them for sale directly to the company or person involved, at prices far beyond the cost of registration. Alternatively, they can keep the registration and use the name of the person or business associated with that domain name to illicitly solicit business for their own sites.

Taking into consideration the increasing business value of domain names on the Internet, it appears that disputes between the cybersquatters and businesses or individuals whose names and/or marks have been registered in bad faith have increased at an accelerated pace.

In South Africa, a dispute resolution mechanism specifically tailored and dedicated for the dot ZA domain has been introduced. This mechanism, known as "ZADRR", was adopted 22 November 2006,[73] to provide a dispute resolution process which can be administered online. The entire process could take less than 55 days to complete.[74]

The South African Institute of Intellectual Property Law (SAIIP), established in 1954 and representing some 140 patent attorneys, patent agents and trade mark practitioners in South Africa,[75] applied to the Department of Communications to become an accredited ZADRR dispute resolution provider and its application for accreditation was approved in early 2007. Prior to such accreditation, the only possible action which could be taken against cybersquatters of the dot ZA domain name was to institute court proceedings for trade mark infringement in South Africa.

This new procedure administered by SAIIPL is very similar to the procedure followed by the WIPO in its administration of ICANN's Uniform Dispute Resolution Policy. The procedure was introduced in South Africa on 1 April 2007. The ZADRR permits complainants to file a dispute with a service provider, specifying the reasons why the concerned domain name registration constitutes an abusive or offensive registration. The respondent is offered the opportunity to defend itself against the allegations.

---

typographical errors made by users when entering domain names into their web browsers. Some common examples of typosquatting include: (a) the omission of the "dot" in the domain name: wwwsite.com; (b) a common misspelling of the intended site: cite.com; (c) a differently phrased domain name: sites.com; and (d) a different top-level domain: site.org. Secondly, there is "renewal snatching," where cybersquatters rely on the fact that trademark holders often forget to renew or re-register their domain names. If the owner of a domain name does not re-register the domain name prior to expiration, then the domain name can be purchased by anybody, and cybersquatters will snatch up a domain name as it becomes free. See <www.cybersquatting.com>, last accessed 15 June 2011.

73 Electronic Communications and Transactions Act (25/2002): Alternative dispute resolution regulations, Government Gazette No. 29405, 22 November 2006, p. 3. Available at <www.domaindisputes.co.za/downloads/AlternativeDisputeResolutionRegulations.pdf>, last accessed 15 June 2011.

74 Bowman Gilfillan website. Available at <www.bowman.co.za/ZADRR/Index.asp>, last accessed 15 June 2011.

75 South African Institute of Intellectual Property Law, Domain Name. Available at <www.saiipl.org.za/domain-name-faq.htm>, last accessed 15 June 2011.

The dispute resolution service provider appoints one or three adjudicators who will render a decision based the relatively swift documents only procedure taking into account the applicable regulations and past ZADRR precedents.[76] Either party may appeal a decision.

The appeal panel will consider appeals on the basis of a full review of the matter and may also review procedural matters. However, no monetary damages are awarded in the ZADRR procedure, and no injunctive relief is available. The accredited domain name registries, which have agreed to abide by the ZADRR, implement a decision upon the lapse of ten days, unless the decision is appealed. The adjudicators' decisions are binding in the sense that accredited registries are bound to take the necessary steps to enforce a decision, such as transferring the disputed domain name.

4.2 South Africa's Onlineombud

The Onlineombud initiative is another South African ODR initiative targeting consumer disputes. Onlineombud offers an all encompassing range of services in the field of consumer relations and complaint management. Their services include advice on and assistance with implementing the CPA, as well as a dispute resolution service that focuses on restoring relationships to the benefit of all stakeholders: consumers and businesses.[77] Their ODR services are offered under two schemes:[78] (a) online Quick view;[79] and (b) online recommendation.[80] Offline mediation and arbitration are also available if the online scheme ultimately fails.[81]

Onlineombud considers disputes filed by consumers against service providers who may be private individuals, small businesses with a turnover of less than one million SAR, a beneficiary of a trust or estate, credit guarantor, a person who suffered monetary loss

76 The listed number of adjudicators is sixty-six. See <www.domaindisputes.co.za/adjudicators.php>, last accessed 15 June 2011. Past decisions and precedents are published online. Available at <domaindisputes.co.za/decisions.php?tag=6>, last accessed 15 June 2011.

77 See <www.onlineombud.com>, last accessed 15 June 2011.

78 Regarding the procedures and jurisdiction of the Onlineombud processes, see <www.onlineombud.com/procedures.html>, last accessed 15 June 2011.

79 "Quick View" is a process based on the information provided by the parties. It aims at assessing the probabilities and any legal considerations. A suggestion is then made as to how the parties ought to best resolve the complaint. The suggestion is not binding on either party unless they both accept it. See <www.onlineombud.com/complaint_process.html>, last accessed 15 June 2011.

80 "Recommendation" is a phase two process which is only applicable if a resolution is not achieved following the issuing of a Quick View. According to the "Recommendation" process, Onlineombud will gather such further information (investigate) as is necessary to assist in the resolution of the complaint. Onlineombud will then issue a recommendation determining the most appropriate resolution of the complaint. If a recommendation is made against a party that accepts Onlineombud's procedures, and it is accepted by the customer, the recommendation will be contractually binding on the subscriber. See <www.onlineombud.com/complaint_process.html>, last accessed 15 June 2011.

81 See <www.onlineombud.com/complaint_process.html>, last accessed 15 June 2011.

due to the service provider, or a person who failed to resolve a dispute through direct negotiations with the service provider.[82]

Regarding the jurisdiction of the Onlineombud services, they shall not consider the following disputes: (i) disputes of an amount exceeding one million SAR or is part of a larger claim, or if together with another claim that may be filed by the complainant against the service provider would exceed one million SAR unless the other claim is unrelated; (ii) complaints pertaining to acts that occurred more than three years prior to filing with Onlineombud; (iii) complaints pending before any other ombuds procedure, court, or tribunal; and (iv) with respect to matters falling outside the ambit of the National Credit Act No. 34 of 2005 (NCA), complaints relating to the pricing policy of the service provider and complaints pursued by the complainant in an unreasonable or abusive manner.[83]

With respect to the Onlineombud procedures, several principles merit a mention in this context.[84] First, by resorting to such procedures, both the service provider and the consumer or complainant shall not be subject to any prescription during the resolution process.[85] Secondly, any exchanged correspondences, communications, documents or recommendations during the processes are privileged and may not be invoked or submitted in any court action.[86] Thirdly, if a matter that falls within the NCA is resolved by agreement or recommendation, the resolution may be issued in the form of a consent order before the court or NCA tribunal. Fourthly, in order to encourage service provider participation, if the latter did not provide the information requested by Onlineombud in a timely manner, Onlineombud shall assume that the evidence is against the service provider and shall make a recommendation accordingly. Finally, Onlineombud may dismiss a complaint if (i) the complainant misled the Onlineombud, or failed to cooperate or respond to any request for information within a reasonable time; (ii) Onlineombud is unable to resolve the complaint or a dispute cannot be resolved on a balance of probabilities; and (iii) if it appeared that the complaint falls out of the jurisdiction of Onlineombud.

The above mentioned initiatives clearly indicate that whilst South Africa has taken the lead in sector specific disputes, namely domain names and consumer relations, other African States are quite ready and near to ODR implementation. For example, unlike South Africa, other ICT ready States such as Tunisia, Morocco, and Egypt have not yet imple-

82 See <www.onlineombud.com/procedures.html>, last accessed 15 June 2011.

83 *Id.*

84 *Id.*

85 *Id.* This is actually a form of a "tolling agreement" or a "clock-stopper" where both parties have agreed to waive any claim of expiration of a statute of limitations that may arise due to the lapse of time spent on Onlineombud processes. This certainly allows both parties a party additional time to assess and determine the legitimacy and viability of their claims and/or the amount of their damages without the necessity of filing an action. Such waiver is only applicable throughout the period of utilizing Onlineombud processes.

86 This encourages full transparency and ensures that both parties will not be disadvantaged by participating in such processes in utmost good faith.

mented any specific regulation for domain name dispute resolution and there exists no proper authority acting as a dispute resolution provider. However, they are members of international initiatives which open the path for the licensing or accreditation of ODR providers in the context of domain name disputes pertaining to those countries.

Nevertheless, it should be noted that the Uniform Domain Name Dispute Resolution Policy (UDRP), adopted by the Internet Corporation for Assigned Names and Numbers (ICANN) on 26 August 1999 and based on recommendations made by the World Intellectual Property Organization (WIPO), provides a mechanism for resolving a domain name dispute regardless of the location of the registrar, the domain name registrant, or the complaining trademark owner. The UDRP permits complainants to file a case with a resolution service provider, specifying, mainly, the domain name in question, the respondent or holder of the domain name, the registrar with whom the domain name was registered and the grounds for the complaint.

Accordingly, requests concerning .TN, .MA or .EG domain name dispute can be addressed to the WIPO Arbitration and Mediation Center where domain name cases filled are normally concluded within two months, using online procedures.[87] Proceedings administered by the WIPO Center have involved parties from over 144 countries across the world, including several others African countries, and can be seen as a first step to be followed towards Online Dispute Resolution.

5 Conclusion: The Future of ODR in Africa

The above mentioned overview of Africa's ODR potential confirms that, hitherto, Africa is generally outsourcing its ODR systems and schemes to extra-continental providers located in other regions and continents, but extending their services globally to everyone including the African people. In other words, whilst people are increasingly moving their lives online in both African and the Middle East, people are still relying on ODR providers located elsewhere. This has certainly impacted the availability of bespoke ODR services. For example, most available ICT applications, software, and providers do not, understandably, cater for African and Arabic languages and culture. However, with the proliferation of ADR centres throughout Africa, over twenty African States have, usually under a national chamber of commerce, established ADR centres since 1995.

This may imply that African governments may step-in to incentivize and promote ODR by adopting and encouraging pilot ODR projects, especially in the e-government, telecommunications, and IT arenas since it may be argued that they are the most ODR

87 World Intellectual Property Organization, World Intellectual Property Organization Supplemental Rules for Uniform Domain Name Dispute Resolution Policy, In effect as of 14 December 2009, Online publication. Available at <www.wipo.int/amc/en/domains/supplemental/eudrp/#4>, last accessed 15 June 2011.

oriented sectors appropriate for governmental intervention given the regulatory role of African governments.

To that effect, in so far as disputes associated with e-government are concerned, governments may wish to establish and operate, or simply hire an established ODR provider that would cater for such administrative disputes that may arise in a G2C and G2B context.[88] In support of such approach, it is submitted that African and Middle Eastern States are generally comfortable with the State interventionist *modus operandi*. Moreover, the absence of adequate ADR schemes that tackle such administrative and governmental disputes warrant the utilization of ODR schemes that would ultimately offer an efficient system for resolving administrative disputes arising from e-government dealings, especially in light of the general inefficiencies and delays in the African and Middle Eastern judicial system.[89]

That said, and taking into consideration the tidal wave of political unrest in some African States as well as the recurring disputes arising from diverse election processes, ODR may offer novel and efficient schemes to resolve electoral disputes, especially that the failure to resolve election controversies peacefully and in a timely manner can lead to conflict escalation, which would threaten the democratic process and political stability of the State. In such context, ODR can truly offer affordable, geographically and legally available processes that could produce efficient, unprejudiced, and impartial results within a short time frame in many instances. This would ultimately strengthen credibility and guarantee public trust in neutral schemes that produce unbiased results.

On a different note, amongst the new initiatives that may qualify as ODR precursors in Africa, is the "Sierra-Leone Peacetones" project.[90] This project aims at the following: (i) supporting talented and hardworking artists living in remote and developing communities through the use of digital media and e-commerce; (ii) uniting legal, technical, and business expertise to help musicians in frontier countries obtain economic and legal equality; (iii) guiding musicians in learning how to access legal resources and the global market place; (iv) educating diverse communities on how to build their own economic bridges, access available global resources, and resolve their own disputes;[91] and (v) setting up online businesses for artists across the world and promoting them through social networking sites to sell their work online. It is envisaged that a certain percentage of the revenues shall be is invested by artists in their communities in the form of development projects.

88 G2C denotes "Government to Consumers" and G2B denotes "Government to Business."

89 The well established legal maxim reads "Justice Delayed is Justice Denied". In other words, legal and judicial redress should be timely and swift to avert the grave injustice inflicted as a result of undue delay. Such maxim which is often attributed to William Gladstone, finds its origins not only in general principles of law and justice, but has also been enshrined in the "Magna Carta," where clause 40 reads, "[…] to no one will we refuse or delay, right or justice".

90 See <peacetones.org/peacetones-sierra-leone/>, last accessed 15 June 2011.

91 This is clearly an area where ODR could be most beneficial.

By and large, whilst African States are developing at different degrees given the intertwined matrix of techno-legal, socio-political, and economic infrastructures, ODR is no longer a distant dream, but rather a very much a proximate reality. South Africa has taken the lead with its two ODR initiatives in domain names and consumer disputes, and more States, such as Egypt, Morocco, Tunisia, Nigeria, Sierra-Leone, etc. are expected to follow suit in the near future. However, training, trust, and expertise remain an indispensable necessity for the proliferation of ODR systems in Africa.

Whilst certain techno-legal, socio-political, and economic challenges exist to the development of ODR in Africa, it is submitted that the future of ODR in Africa is not uncertain with respect to ultimate implementation. The uncertainty pertains to those amenable and competing sectors, which could form a strong entry point for ODR in Africa.

In conclusion, it is submitted that the robustness of Africa's lust for adequate and efficient dispute resolution processes shall be, in the near future, fulfilled by ODR schemes, which could be court-annexed or privately driven trusted systems.