Data Protection Regimes in Africa: too far from the European 'adequacy' standard?

Alex Boniface Makulilo*

Abstract

- In 2010, the Research Centre on IT and Law, University of Namur, Belgium, also known by its French acronym as the CRID, undertook evaluation of data protection legislation in the four African jurisdictions: Burkina Faso, Mauritius, Tunisia, and Morocco.
- The CRID carried out the evaluation under a consultancy agreement with the European Union. None of these jurisdictions passed the 'adequacy' test of the European Data Protection Directive 95/46/EC.
- In this article, I discuss the African data protection regime in the context of the CRID's reports and assess the implications of such findings to the future development of data privacy law in Africa.

Current state

Over four decades of the development of data protection laws, the world has witnessed data protection regimes finally arriving in Africa. At present, there are eleven African countries out of 54 with comprehensive data protection legislation. These are Cape Verde (22 January 2001), Seychelles (24 December 2003), Burkina Faso (20 April 2004), Mauritius (17 June 2004), Tunisia (27 July 2004), Senegal (15 January 2008), Morocco (18 February 2009), Benin (27 April 2009), Angola (17 June 2011), Gabon (25 September 2011), and Ghana (10 February 2012). At the same time, in an attempt to harmonize the emerging national data protection legislation and perhaps to prevent disruption of flow of personal data, in 2010 the Economic Community of West African States (ECOWAS) adopted a sub-regional framework for its member states.[1] In contrast, in the same year the East African Community (EAC) adopted data privacy recommendations for its members.[2] While these recommendations do not stipulate substantive data protection principles as is the case with most other sub-regional and regional codes of data protection, they intend to encourage the member states to align with the international best practices. The Southern African Development Community (SADC) and the African Union (AU) are still considering drafts of data privacy instruments.[3]

As is the case elsewhere, the emerging data protection regime in Africa is partly influenced by the European Union Data Protection Directive 95/46/EC. The international regime for the transfer of personal data contained in the Directive 95/46/EC, particularly Articles 25–26, is most frequently cited by commentators as one of the forces behind this development.[4] Article 25 of the EU Directive restricts the transfer of personal data to third countries, that is non EU/EEA countries, unless such countries afford an 'adequate' level of data protection. However, under Article 26 of Directive 95/46/EC personal data may still be transferred from EU/EEA to third countries even if such countries fail to pass the 'adequacy' test. Yet, this is only a limited option as it is a derogation from the main rule in Article 25 of the Directive.

Undoubtedly, the requirements of Article 25 of Directive 95/46/EC necessitated the above four African

* Alex B. Makulilo is a lecturer at the Faculty of Law, Open University of Tanzania. E-mail: alex.makulilo@googlemail.com.

1 ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection 2010. Currently ECOWAS has 15 members: Benin, Burkina Faso, Cape Verde, Côte d'Ivoire, Gambia, Ghana, Guinea, Guinea Bissau, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone, and Togo.

2 EAC, Legal Framework for Cyber Laws, (Phase I) November 2008 (adopted on 7 May 2010 during the 2nd extraordinary meeting of the Community's Sectoral Council on Transport, Communications and Meteorology). Currently EAC has 5 members Kenya, Uganda, Tanzania, Rwanda, and Burundi.

3 SADC Data Protection Model-Law 2012 and AU, Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa, Version 01/01.2011 respectively.

4 See eg LA Bygrave, 'Privacy and Data Protection in an International Perspective' (2010) 56 Scandinavian Studies in Law 165–200, at 194.

countries to seek EU accreditation of their data protection legislation. The applications for accreditation triggered the assessment of 'adequacy'. In this context, the European Commission in 2010 mandated the Research Centre on IT and Law, University of Namur, Belgium, to research the level of data protection in the four African countries; these reports raise questions about the methodology used to make adequacy decisions, and its implications for policy making in third countries.

The 'adequacy' standard under Directive 95/46/EC

The default rule for the international transfer of personal data in the Directive is provided in Art 25(1). This provision states:

> The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

The above provision sets out an 'adequate level of protection' as the basic condition for transfer of personal data from the EU/EEA to a third country, that is a country outside the EU/EEA region. However, the Directive does not define what is meant by 'adequate level of protection'. Yet it provides criteria of its assessment. Article 25(2) sets out these criteria in the following terms:

> The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied within that country.

What clearly emerges from here is that Article 25 is not directed so much to the general provisions of the law in a third country, but to the actual level of protection which will be accorded in a particular case.[5] This view is cemented by the Article 29 Working Party who says, 'Article 25 envisages a case by case approach whereby assessment of adequacy is in relation to individual transfers or individual categories of transfers.'[6] Usually this assessment lies first with the data exporters and second with national data protection authorities in the EU/EEA.[7] However, the European Commission is empowered under Article 25(6) to make general determinations of 'adequacy' which are binding on EU/EEA member states.[8] In comparison with data exporters and national supervisory authorities, the Commission is in a better position to assess the adequacy of data protection.[9] Such a holistic approach is cost efficient.[10] Moreover, it relieves member states, as they do not have to assess the same cases, and differences between national assessments can be avoided.[11] Similarly, this approach increases certainty and predictability for data transferors.[12]

The effect of the Commission's positive determination is to allow free flow of personal data from the EU member states as well as EEA member countries (Norway, Liechtenstein, and Iceland) to that third country without any further safeguard being necessary.[13] Currently the European Commission has recognized Switzerland, Canada, Argentina, Guernsey, the Isle of Man, Jersey, Australia, the Faeroe Islands, Andorra, Israel, Uruguay, the US Department of Commerce's Safe Harbor Privacy Principles, and the transfer of Air Passenger Name Record to the United States' Bureau of Customs and Border Protection as providing adequate protection. However, a negative determination of adequacy of protection bars the free flow of information to a third country under Article 25(4) of

5 F Aldhouse, 'The Transfer of Personal Data to Third Countries under EU Directive 95/46/EC' (1999) 13(1) International Review of Law Computers & Technology 75–79, at 76.

6 Article 29 Data Protection Working Party, 'Discussion Document: First Orientations on Transfers of Personal Data to Third Countries—Possible Ways Forward in Assessing Adequacy', XV D/5020/97/ EN, WP 4, (adopted on 26 June 1997), 1.

7 LA Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (The Hague/London/New York: Kluwer Law International, 2002), 81; see also Article 29 Data Protection Working Party (n 6), at. 2.

8 Bygrave (n 7), supra; note also that the Commission does not make such decisions on its own but with input from (i) the Data Protection Working Party(which may deliver a non-binding opinion on the proposed decision(Art. 30(1)(a) & (b); the Article 31 Committee (whose approval of the proposed decision is necessary and which may refer the matter to the Council for final determination (Art. 31(2)); and (iii) the European Parliament(which is able to check whether the Commission has properly used its powers), see Bygrave (n 7) fn 317; see also European Commission., 'Commission decisions on the adequacy of the protection of personal data in third countries' <http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm>, accessed 13 August 2012.

9 L Kong, L., 'Data Protection and Transborder Data Flow in the European and Global Context' (2010) 21(2) The European Journal of International Law (EJIL) 441–56, at 445.

10 Ibid.

11 Ibid.

12 Ibid.

13 I Lloyd, *Information Technology Law* (6th edn, New York: Oxford University Press), 192.

Directive 95/46/EC. It is also important to bear in mind that in all cases where a member state or the Commission considers that a third country does not ensure an adequate level of protection of personal data within the meaning of Article 25(2), such information is required to be shared across member states. Yet, it is doubtful if in the former case the notification may have a binding effect on the other member states.

The second set of rules of international transfer in the Directive relates to the derogations from the default rule. These are provided in Article 26. They apply where a third country does not provide an 'adequate level of protection' to transfer of personal data. Article 26(1) lays down six criteria in the alternative to be fulfilled before a transfer of personal data to such a third country can be permitted, that is where (a) the data subject has given consent unambiguously to the proposed transfer; or (b) the transfer is necessary to perform certain contracts between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request; or (c) the transfer is necessary for the conclusion or performance of a contract in the interests of the data subject between the controller and a third party; or (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise, or defense of legal claims; or (e) the transfer is necessary to protect the vital interests of the data subject;[14] or (f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest.

Article 26(2) provides another possibility of derogation. In this case, transfer of personal data may be authorized by a member state where the data controller adduces 'adequate safeguards' with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses. The 'adequate safeguards' referred to in this provision are not in any way less than the 'adequate protection' standard which consists of a series of basic data protection principles together with certain conditions necessary to ensure their effectiveness.[15]

Also to ensure that these arrangements do not weaken the level of protection of personal data, a member state which has so authorized transfer of personal data in accordance with Article 26(2) is required to notify the other member states and Commission.[16] If upon such notification a member state or the Commission objects to the assessment on justified grounds, the latter will take appropriate measures and comply with it.[17] Finally, the Commission may decide that certain standard contractual clauses offer sufficient safeguards in terms of Art 26(2).

Evaluation of 'adequacy' in practice

As pointed out, the European Commission is the institution mandated to make general decisions over 'adequate level of protection' provided for in a third country. However, in exercise of this power, more often the Commission receives non-binding opinion from the Article 29 Working Party. The latter had developed a methodology of assessment of 'adequacy' comprised in the two sets of documents namely, 'First Orientation on Transfers of Personal Data to Third Countries: Possible Ways Forward in Assessing Adequacy'[18]—the WP 4—and 'Working Document on Transfer of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive'[19]—the WP 12. However, the latter is more significant and it is currently regarded in Europe as authoritative.

The WP 12 sets out two levels of assessment of 'adequate level of data protection' with regard to international transfer of personal data to third countries. The first level of assessment relates to 'content' principles while the second relates to 'procedural/enforcement'. In principle, the former are modified versions of the data protection principles contained in the Directive 95/46/EC while the latter mirror the enforcement mechanisms envisaged to a large extent under chapter VI of the Directive.

Content principles

The WP 12 has six main content principles for assessing the 'adequacy' level of data protection in a third country. The first is the purpose limitation principle. This requires that data should be processed for a specific purpose and subsequently used or further communi-

14 The expression 'vital interest' of the data subject has a restrictive meaning to mean 'which is essential for the data subject's life', see Directive 95/46/EC, Recital 31.

15 Article 29 Data Protection Working Party, 'Working Document on Transfer of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive', DG XV D/5025/98/WP 12, (adopted on 24 July 1998), 17.

16 Directive 95/46/EC, Art 26(3).

17 Ibid.

18 Article 29 Data Protection Working Party (n 6).

19 Article 29 Data Protection Working Party (n 15).

cated only insofar as this is not incompatible with the purpose of the transfer. The exemptions to this rule would be those necessary in a democratic society on one of the grounds listed in Article 12 of the Directive. The second principle is called the data quality and proportionality principle. It requires that data should be accurate and, where necessary, kept up to date. Data should be adequate, relevant, and not excessive in relation to the purposes for which they are transferred or further processed. The third principle is the transparency principle. It states that individuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country, and other information insofar as this is necessary to ensure fairness. The only exemptions permitted should be in line with Articles 11(2) and 13 of the Directive. The fourth principle is called the security principle. It provides that technical and organizational security measures should be taken by the data controller that are appropriate to the risks presented by processing. Any person acting under the authority of the data controller, including a processor, must not process data except on instructions from the controller. The fifth principle relates to rights of access, rectification, and opposition. According to this principle, the data subject should have a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to the processing of the data relating to him/her. The only exemptions to those rights should be in line with Article 13 of the Directive. The sixth principle is about restrictions on onward transfers. It provides that further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (ie the recipient of the onward transfer) is also subject to rules affording an adequate level of protection. The only exceptions permitted should be in line with Article 26(1) of the Directive.

Besides the above general principles, WP 12 sets out by way of examples, additional principles to be applied in specific types of data processing. These include the sensitivity principle providing that where 'sensitive' categories of data are involved (those listed under Article 8 of the Directive), additional safeguards should be in place, such as a requirement that the data subject gives his/her explicit consent for the processing. The other principle involves direct marketing. It requires that where data are transferred for purposes of direct marketing, the data subject should be able to 'opt out' from having his/her data used for such purposes at any stage. Finally, there is the automated individual decision principle. This principle states that where the purpose of the transfer is the taking of an automated decision in the sense of Article 15 of the Directive, the individual should have the right to know the logic involved in this decision, and other measures should be taken to safeguard the individual's legitimate interest.

Procedural requirements

The WP 12 identifies three main objectives of a data protection system. The first is the delivery of a good level of compliance with the rules. A good system is generally characterized by a high degree of awareness among data controllers of their obligations, and among data subjects of their rights and means of exercising them. The existence of effective and dissuasive sanctions can play an important role in ensuring respect for rules, as of course can systems of direct verification by authorities, auditors, or independent data protection officials. The second objective is the provision of support and help to individual data subjects in the exercise of their rights. The individual must be able to enforce his/her rights rapidly and effectively, and without prohibitive cost. To do so there must be some sort of institutional mechanism allowing independent investigation of complaints. The third objective is the provision of appropriate redress to the injured party where rules are not complied with. A good system of enforcement must comply with the above objectives.

The 'adequacy' standard in the four African jurisdictions

Burkina Faso

On 17 May 2010, CRID released its report on the analysis of the adequacy of protection of personal data provided in Burkina Faso.[20] Interestingly, it refrained from giving its conclusion whether Burkina Faso provides an 'adequate' level of protection of personal data. The CRID's report partly reads, '... the authors of the present report want to insist on the fact that, on the basis of the content of the report, they are not able to conclude that the protection of personal data in Burkina Faso is—or not—adequate. A more clear vision should be possible after the modification of the

20 CRID, Analysis of the Adequacy of Protection of Personal Data Provided in Burkina Faso (2010).

Data Protection Act and the analysis of such modification.'[21]

According to the CRID's report, the Burkina Faso Data Protection Act 2004 was in the process of being modified, hence CRID could not assess the country's level of 'adequacy' of protection of personal data. Surprisingly, it continued to make an assessment of the enforcement mechanism based on the same piece of legislation it declined to evaluate. Yet, there is no sound reason advanced by CRID in the report for this partial assessment. As alluded to, the WP 12 has two sets of criteria for evaluating the 'adequacy' of data protection in a third country. These are content principles as well as procedural/enforcement mechanisms. An 'adequacy' assessment has to take into account both sets of these criteria. It is interesting to note that at the end of its analysis of the enforcement mechanism under the Data Protection Act, CRID concluded that the Burkina Faso's data protection authority is structurally and financially independent.[22] However, it noted that the people's level of awareness in Burkina Faso is still not too high.[23] Concomitantly, there is no good level of compliance with the rules.[24] Yet, in another disclaimer which defeats CRID's partial assessment, the report reads, 'in the opinion of the authors, time should be given to this (modified) text, in order for it to be applied and for Burkina Faso to live with it. Giving adequacy conclusions without the existence of case law and a higher awareness seems not opportune as the existence of actual enforcement mechanisms is an important part of the criteria to meet before being possibly considered as a country offering an adequate protection in the sense of article 25 of the European Directive 95/46.'[25] Arguably, it was less beneficial for CRID to carry out a partial assessment when it was not sure if the provisions assessed would not be modified by a new law. Moreover, as it correctly stated, sufficient time is required to observe the actual practice of the modified Act, hence CRID's assessment was premature.

Mauritius

On 30 April 2010 CRID released its final report on the analysis of the adequacy of protection of personal data provided in Mauritius.[26] The overall outcome of this assessment is presented in four aspects. First, the adequacy conclusion with respect to the public sector is that the Mauritian data protection system is far from being considered to fully comply with the WP 12 requirement. This is largely due to the broad range of its exemption regime with no relevant justification. The report identifies, for example, the exemption of 'information available to the public' as well as weaknesses as regards 'criminal and taxation' and 'regulatory activities' to be the main areas of concern. At the same time the CRID noted that some activities have been exempted from the application of the basic principles of data processing yet remained subject to the provisions of the Act dealing with the same principles.

Second, the adequacy conclusion with respect to the private sector is that the Data Protection Act 2004 affords a wider protection. Nevertheless, there are limitations on the exemption of the data subject's right of access when the processing is in connection with employment or in matter of 'social work'. Moreover, there are no restrictions in the matter of automated individual decisions.

Third, as for the enforcement mechanisms, the issue of registration procedure is considered to be problematic since it is burdensome. Moreover, there is little guarantee that data subjects might exercise their rights effectively and without prohibitive costs.

The fourth conclusion is that the Mauritian Data Protection Act contains (too) many examples of poor drafting and contradictions. As a result many aspects are difficult to understand—sometimes even have no sense—or are difficult—or even impossible—to apply. The CRID's report emphasizes that the poor drafting aspect should not be underestimated at the time of assessing the adequacy of the data protection system in Mauritius.

The above adequacy conclusions have taken into account specific issues. In particular, the CRID was concerned with the exception to the rule 'information available to the public' which appears dominantly in the Act. This rule is too broad and without any relevant justification. As a result it has undermined almost all the content principles in the WP 12. Yet, interestingly the CRID observes that with respect to 'the exemption to the right of access of data subject in the health and social work field, such exemption though not compliant with the WP 12 requirements, is mostly problematic at national level, and does not raise much issue with respect to European personal data protection'.[27] This

21 Ibid, at 54.
22 Ibid.
23 Ibid.
24 Ibid.
25 Ibid.
26 CRID, Analysis of the Adequacy of Protection of Personal Data Provided in Mauritius (2010).
27 Ibid, at 102.

suggests that it is the protection of European residents' interests that matters most in the assessment of 'adequacy', rather than the interests of residents of a third country.

With respect to the international transfer of personal data, CRID found that such regime is also problematic. The adequacy issue here is that every transfer of personal data outside Mauritius requires the authorization of the data protection commissioner. This is regardless of whether such country affords an adequate level of protection hence making the regime of international transfer highly restrictive.

Similarly, at the time of assessment there was no case law or any decisions decided on the basis of the Data Protection Act. Accordingly, it was difficult for the CRID to have a thorough picture of how the Act functions in practice.

The rest of the provisions of the Mauritian Data Protection Act were found to be compliant with the WP 12. However, taken in their totality, such provisions could still not warrant an adequacy clearance.

Tunisia

On 22 December 2010 CRID released its final report on the analysis of the adequacy of protection of personal data provided in Tunisia.[28] The overall outcome of this assessment states in part, '... in our exclusive personal view, the Tunisian regime regarding the protection of personal data is to be considered *inadequate*, at the present time, and on the basis of our comprehension of the Act in force.'[29]

In arriving at the above conclusion, CRID found a number of shortcomings in the whole of the Tunisian data protection system. One such shortcoming rests upon the territorial scope of the Data Protection Act 2004. It found that the Tunisian Act does not provide for a specific provision on the territorial scope of the law. However, section 22 of the Act clearly states that the physical person or the representative of the legal person wishing to perform personal data processing and their agents must have Tunisian nationality, have a residence in Tunisia, and have a blank criminal record. According to this provision, a foreign person or legal entity will neither be a controller or a processor of personal data in Tunisia, nor an employee or agent of a controller or processor of such data without violating the Act.[30] At the same time, even a Tunisian citizen who does not have his/her residence in Tunisia shall not be able to be involved in the processing of personal data performed in Tunisia, either as a controller, a processor, or an agent.[31] The CRID emphasizes that section 22 of the Tunisian Data Protection Act is problematic as it restricts foreign persons or companies on the Tunisian territory while at the same time Tunisia is ranking highly as an important offshore destination.[32]

Moreover, the Tunisian Data Protection Act has an extensive derogatory regime. According to CRID, a large number of provisions of the Act are not applicable to public authorities. Section 53 of the Act is cited as the most problematic one as it leads to many exemptions in the Act.[33]

Somewhat related to the above, the CRID found that the derogative regime in the Tunisian Act undermines significantly the requirement of transparency. Often data subjects are not aware of the existence of data processing by public authorities. Similarly, when authorization by the data protection authority is required for certain types of processing (eg data relating to health or video surveillance purposes), the Act does not provide for an obligation of informing of the data subject, raising an issue of transparency in those cases.[34]

The data subject's right of access with regard to the processing carried out by the public persons is highly compromised. According to CRID, public persons are exempted from providing a right of access in some cases which might go beyond the cases listed in Article 13 of the Directive.[35]

Another problematic area is on the Tunisian international onward transfer regime. The CRID found the regime to be highly restrictive. This is because it requires authorization of the data protection authority for every transfer of personal data outside Tunisia. There is no exception to this rule even to countries possessing an adequate level of protection of personal data.

With regard to sensitive data, the general prohibition to process personal data related to criminal offences is held to be unrealistic and a dead letter since professionals (eg lawyers, bailiffs, etc.) process these data as part of their activities. Similarly, CRID found that the absence of any guarantees as to the processing of sensitive data by public persons is wholly unsatisfactory.

Moreover, Tunisia has neither a regulation nor any provision in the Data Protection Act on the issue of

28 CRID, Analysis of the Adequacy of Protection of Personal Data Provided in Tunisia (2010).

29 Ibid, at 123.

30 Ibid, at 33.

31 Ibid.

32 Ibid, at 34 & 63.

33 Ibid, at 27–31.

34 Ibid, at 115.

35 Ibid, at 117.

automated individual decision. Due to this, CRID concludes that the Tunisian regime of data protection fails to pass the adequacy requirement to that extent.

The procedural/enforcement mechanisms have their shortcomings too. In particular, the CRID is concerned with the independence of the Tunisian data protection authority. Members of the authority drawn from the public sector lack guarantees. Moreover, the authority financially and structurally is linked to the Ministry of Justice and Human Rights. Similarly, the exemptions on public persons have constrained the support and help to individual data subjects.

There are two other considerations which the CRID took into account in its findings. First, the Tunisian data protection authority was only recently established. At the time of assessment it had not yet issued any regulatory document such as recommendations, guidelines, decisions, etc. Second, for the same reason, there were no decided cases in relation to the application of the Act hence it was difficult to assess the application of the law in practice. Moreover, the interpretation of the law has been made somewhat difficult due to poor drafting of the Act in several places.

Keeping aside the shortcomings discussed above, the rest of the provisions of the Tunisian Data Protection Act were found to be compliant with the WP 12. Yet, when considered together these provisions do not constitute an adequate level of protection of personal data.

Morocco

On 13 August 2010 CRID released its final report on the analysis of the adequacy of protection of personal data provided in Morocco.[36] The CRID holds that the issue of protection of personal data in Morocco is relatively new. The legislation on data protection was adopted largely to fill the legal vacuum in this area for the purposes of offshoring activities in Morocco. Due to this, and also the fact that the Moroccan data protection authority officially started to function on 2 September 2010, it was premature for CRID to make a general conclusion on whether the Moroccan data protection system provides an adequate or inadequate level of protection.

However, a theoretical evaluation of the Moroccan data protection legislation revealed a number of shortcomings. As observed by one of the authors of the CRID's report for Morocco, data concerning sex life are not considered as sensitive, though the definition of 'sensitive data' closely follows the European one.[37] This is due to the Muslim character of the Moroccan State.[38] However, it is surprising the Legislator has recognized 'philosophical and religious beliefs' as sensitive data, while the processing of this type of data occurs regularly in a variety of situations in Morocco.[39]

Although the principle of transparency in the Moroccan data protection legislation is held to be compliant with the WP 12, adequacy issues have been raised with respect to exceptions to the disclosure requirement of processing in the context of 'open networks'. First, the concept of 'open networks' is not defined in the Moroccan Act to help ascertain the scope of exemption. Second, the law imposes upon data controllers the duty to inform data subjects about collection of their personal data in 'open networks' unless the latter already know that such data would circulate without security guarantee or may be used by unauthorized third parties. The CRID finds that the formulation of this provision is awkward. Similarly the consultant noted that it is difficult to distinguish 'a person who already knows' and 'a person who does not know' in the so called 'open networks'. The CRID is also concerned by the formulation of Morocco's provision on transparency for being contradictory. This is due to the fact that it authorizes a data controller to collect personal data and at the same time it does not impose a duty upon him to inform when he knows that the information collected will be used by third parties whom the Act itself calls unauthorized parties.

Likewise the CRID found that contrary to the European data protection Directive 95/46/EC which places consent on the same level as the other legitimate grounds for processing personal data, the Moroccan Act singles out consent as the only ground for processing. However, it puts the other grounds in an inferior position leading to restriction.

The adequacy of the international transfer of personal data is similarly at issue. The reason is that it always requires the approval of the data protection commissioner. This is irrespective of whether the foreign country provides an adequate level of protection of personal data.

The rest of the provisions of the Moroccan data protection law were found to be compliant with the WP 12. However, these provisions could not satisfy the adequacy clearance criteria.

36 CRID, Analyse du Niveau d'Adequation du Systeme de Protection des Donnees dans le Royaume du Maroc (2010).

37 C Gayrel, 'Data Protection in the Arab Spring: Tunisia and Morocco' (2012) 115 Privacy Laws & Business International Report 18–20, at 20.

38 Ibid.

39 Ibid.

Flawed determinations?

Although the Article 29 Working Party has attempted to lay down legally non-binding rules for assessment of 'adequate level of data protection' in third countries, specifically those found in WP 4 and WP 12, in practice it has taken into account extraneous latent considerations not envisaged by the Directive itself. For example, the Article 29 Working Party commissioners have considered and hence taken on board political considerations in the assessment. In their view 'some third countries might come to see the absence of a finding that they provided adequacy protection as politically provocative or at least discriminatory, in that the absence of a finding is as likely to be the result of their case not having been examined as of a judgment on their data protection system.'[40] Performing the adequate assessment on these fears has rendered 'political considerations an obstacle for a sound evaluation, as not placing a country on the white list is similar to blacklisting it'.[41] Since CRID deployed the PW 12 in its analyses, it is doubtful if it was able to overcome these fears.

However, in mitigating the chances of an occurrence of diplomatic and political tensions with third countries, the EU has in most cases awaited requests from third countries to initiate the process of accreditation.[42] Concomitantly where at first instance the Commission finds problems with the data protection regulations and practices in a third country, it normally engages such countries and facilitates improvement of their regulations and practices until a required level is reached. In that way the Article 29 Working Party more often adopts its official opinion on the level of adequacy after the third countries have addressed a number of areas of concern. Because of this strategy, most of its adopted opinions have had favourable outcome on third countries except the US Safe Harbor Agreement and the Passenger Name Records.

At the same time, where the Article 29 Working Party had a negative opinion as to the 'adequate level of data protection' in a third country, it used 'neutral' language in its opinion to avoid passing a direct 'verdict' only expressing its dissatisfaction by drawing the attention of the Commission to take into account key areas of concerns when making its decision.[43] However in those cases where an expressed negative opinion is issued, the Article 29 Working Party has never made it public. In this connection Professor Graham Greenleaf argues that, 'there could be significantly more adequacy findings outside Europe if the EU was more pro-active and more transparent about its processes. Where the EU has made positive adequacy decision it has publicized the reasons, but where it has considered "applications" from other countries but concluded that their protections were not yet adequate, it has not generally publicized the reasons for these negative conclusions. There has therefore been much less information available about what does and what does not constitute "adequacy" than is desirable.'[44]

The certification approach is different on some occasions where external consultants had been hired by the Commission to undertake an analysis of the adequacy of data protection in a third country. Here, more direct language, in which a 'spade is called by its name', has been used in those instances of negative findings. This is so, for instance, with the conclusive view of the consultant (CRID) in the case of Tunisia. Perhaps because of this, cases of negative outcome reports on adequacy have either been treated as confidential, allegedly on account of contractual confidentiality clauses between the consultant and the Commission,[45] but in reality to prevent the so called 'political provocation' which the Article 29 Working Party has openly admitted in its guidelines for assessing the level of adequacy of data protection in third countries is a potential risk to diplomatic relations.[46] Yet only rarely have such reports been made public.[47] However, this point need not be exaggerated. In some instances (for instance Burkina Faso, Mauritius, and Morocco) the consultant has used more evasive

40 Article 29 Data Protection Working Party (n 15), at 27; see also Kong (n 9).

41 P Blume, 'Transborder Data Flow: Is there a solution in sight?' (2000) International Journal of Law and International Technology 65–86, at 70.

42 See eg N Ringou, 'Data Protection: European Adequacy Procedure', presentation made in 'Twinning Project IS/2007/ENPAP/JH/01: Strengthening Data Protection in Israel' 30 September 2009, Israel, (23 slides, at slide no.17), <http://www.justice.gov.il/NR/rdonlyres/A31C13F2-3554-4086-929C- 2CFF6D31462C/21169/DataProtectionIsrael.pdf > , accessed 13 August 2012.

43 This was the case, for example, with the determination of 'adequacy' of the Canadian Personal Information and Electronic Documents Act 2000.

44 G Greenleaf, 'Do not dismiss "Adequacy": European Standards entrenched' (2011) 114 Privacy Laws & Business International Report 16–18, at 16–17.

45 This was confirmed to the author of this article by one of the authors of the CRID's reports on 10 January 2012 when the former requested from the latter those reports. The author received similar response from the Commissioner of Data Protection in Mauritius when he requested the same report. However, she promised to send the second report to the author later suggesting that such report may have a favourable assessment from EU authorities.

46 Article 29 Data Protection Working Party (n 15), at 27.

47 See eg CRID, 'Analysis of the Adequacy of Protection of Personal Data provided in Tunisia-Final Report' (2010), <http://alexandrie.droit.fundp.ac.be/GEIDEFile/6544.pdf?Archive=192619191089&File=6544_pdf>, accessed 13 August 2012 and CRID, 'First Analysis of the Personal Data Protection in India-Final Report' (2005) <http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_india_en.pdf>, accessed 13 August 2012.

language but with the same effect of negative determination. Still those reports have been kept confidential.

The other extraneous criterion considered by the Article 29 Working Party in its opinion is the economic importance of a third country to Europe and concomitantly the amount of data of Europeans likely to be transferred there. This can be well demonstrated by the recent clearance of New Zealand by the Article 29 Working Party as providing an adequate level of data protection despite several weaknesses in New Zealand's data protection regime. It is evident that the clearance was prompted by 'New Zealand's relative geographical isolation; the limited EU-sourced data likely to be transferred to New Zealand (which minimizes the problem of onward transfers); and the reciprocal lack of direct marketing into the EU that could be expected from NZ'.[48] It can thus be generally concluded 'that the standard of adequacy is in inverse proportion to proximity, provided that "proximity" is considered to include the economic and social, not only the geographical'.[49] Because the four African jurisdictions have been highly ranked as off-shore destinations for foreign companies, it is doubtful if the CRID was not influenced by such reasons in its assessment.

Similarly, it is significant to note that the Article 29 Working Party has taken into consideration the interests of EU citizens at the expense of those in the third country when assessing the adequacy of the data protection system. Accordingly 'it is the effect of a third party's laws on EU citizens that counts toward adequacy, not the effect on the country's own citizens'.[50] The four CRID reports reflect this view in many places particularly on issues concerning the territorial scope of the legislation, onward transfer, and automated individual decision. It is important to note that on one occasion in its assessment of the Mauritian Data Protection Act, the CRID pointed out that although the exemption with respect to the right of access of the data subject in the health and social work field is not compliant with WP 12, that would be problematic at national level, but does not raise much issue with respect to European personal data protection. This is a clear instance where the effect of a third party's laws on EU citizens takes precedence.

Despite their shortcomings, the CRID's assessments of the 'adequacy' of data protection in the four African jurisdictions raise important questions for the future development of data protection law in Africa. First, the adoption of data protection law in Africa should not be considered a mere exercise of 'cut and paste' of EU law or that of its members. Sufficient debates, discussions, and public consultations must be engaged before such laws are adopted. The South African path is commendable, although it is now taking too long (over 10 years). Second, but somewhat connected to the first point, the drafting of data protection legislation should engage experts. This should not only engage the ordinary draftsmanship departments of the governments, but also experts in the area of data protection law. Third, African governments should not only adopt data privacy legislation for the purposes of attracting foreign investments but also to help their people against unauthorized processing of personal data. Fourth, the CRID's assessments clearly highlight that an adequacy assessment rigorously takes into account how the laws, regulations, guidelines, codes of practice, etc. function in practice. This means that African jurisdictions should not pass a law today and rush for EU accreditation tomorrow. Sufficient time has to pass to allow them to put the law in practice. Early application for EU accreditation, even before the law becomes operational or has not generated any authoritative interpretation, is likely to fail.

doi:10.1093/idpl/ips031
Advance Access Publication 28 November 2012

48 G Greenleaf and LA Bygrave, 'Note entirely adequate but far away: Lessons from how Europe sees New Zealand data protection' (2011) 111 Privacy Laws & Business International Report 8–9, at 9.

49 Ibid.

50 Ibid.