The pioneering journey of the Data Protection Commission of Mauritius

Drudeisha Madhub*

Abstract

- The Data Protection Commissioner of Mauritius faces many challenges as the country upgrades its legal framework to become closer to EU standards.
- The Commissioner's decisions have thus far always respected the law, as well as taking basic jurisprudential principles into account.
- The Commissioner will continue to work to raise the profile of data protection among the citizens of Mauritius, and to meet high standards in issuing decisions and dealing with legal issues that are brought before her.

Introduction

In January 2013, an article was published in this journal where the author wrote the following about the decisions delivered by the Data Protection Commissioner of Mauritius:

> The conclusion drawn from this analysis is that while these decisions reflect the basic data protection principles laid down in the law, they are not consistent to some extent. Similarly such decisions have at times taken into account factors beyond the provisions of the law.[1]

I have thus felt the need to clarify the above statement which, in my humble view, does not correctly reflect the rationale behind each decision. Before proceeding to the decisions, I have deemed it fit to include an overview of the data protection legal and institutional framework in Mauritius for a better understanding of the Commission's role in Mauritian Society.

Background to data protection law in Mauritius

Mauritius has recently made the ICT sector the third pillar of its economy and is aiming to make it the first pillar, which without further justification, shows the importance for the country to have an efficient and internationally recognized data protection regime in place to secure the correct level of investment whilst witnessing a growing Business Process Outsourcing sector. The right to privacy is expressly provided in Sections 3 and 9 of the Constitution and Article 22 of the Civil Code. The Data Protection Act (DPA) was enacted on 17 June 2004 and all of its provisions subsequently came into force on 16 February, 22 May, and 30 July 2009[2] except for Section 17(5). It was not until mid 2010 that the office was equipped with a small administrative staff of four persons and commenced operations. At the time, the Commissioner was the only non-administrative person in the office carrying out the functions provided as follows in Section 5 of the DPA:

(a) ensure compliance with this Act, and any regulations made under the Act;

(b) issue or approve codes of practice or guidelines for the purposes of this Act;

(c) create and maintain a register of all data controllers; and data processors [Amended by Act No. 1 of 2009];

(d) exercise control over all data processing activities, either of its own motion or at the request of a data subject, and verify whether the processing of data is in accordance of this Act or regulations made under the Act;

(e) promote self-regulation among data controllers and data processors;

* Data Protection Commissioner, Republic of Mauritius.

1 Alex Boniface Makulilo, 'Mauritius Data Protection Commission: An analysis of its early decisions'(2013) 3 International Data Privacy Law 131 (the author of this article is referred to throughout as 'the author').

2 Act 13/2004 was proclaimed by Proclamation No. 45 of 2004 and Sections 1 and 2 of Part I, Sections 4, 5(b), (c), (e), (g), (h), (i), and (j) and 6 of Part II came into force on 27 December 2004. Sections 3, 5(a), (d), and (f), 7 to 16 and 18 to 66 were proclaimed by Proclamation No. 5 of 2009 and came into force on 16 February 2009. The amendments made to section 17 through Act 1/2009, were proclaimed on 22 May 2009. Further amendments were made to the Data Protection Act through Act 14/2009, which came into force on 30 July 2009.

(f) investigate any complaint or information which gives rise to a suspicion that an offence, under this Act, may have been, is being, or is about to be committed;

(g) take such measures as may be necessary so as to bring to the knowledge of the general public the provisions of this Act;

(h) undertake research into, and monitor developments in, data processing, including data-matching, data linkage, and information and communication technologies, and ensure that there are no significant risks of any adverse effects of those developments on the privacy of individuals [Amended by Act No. 1 of 2009];

(i) examine any proposal for data matching or data linkage that may involve interference with, or may otherwise have adverse effects on the privacy of individuals and, ensure that any adverse effects of such proposal on the privacy of individuals are minimized;

(ia) co-operate with supervisory authorities of other countries, to the extent necessary for the performance of his duties under this Act, in particular by exchanging relevant information in accordance with any other enactment [Added by Act No. 1 of 2009];

(j) do anything incidental or conducive to the attainment of the objects of, and to the better performance of his duties and functions under this Act. [Amended by Act No. 1 of 2009] (Act No. 14 of 2009)

The Data Protection Regulations came into force on 16 February 2009 and specified the fees to be paid, the forms to be submitted to the office, and the request for access to personal data form to be sent to data controllers by data subjects. The amendments made to the DPA in 2009 were basic and essentially allowed the office to start its operations and did not aim to render the DPA internationally compliant, since the Commissioner was advised to wait for EU expert opinion on the matter which came in 2010 through the Report of the Centre de Recherche Informatique et Droit (CRID) of the University of Namur, Belgium.

The CRID, appointed by the European Commission, produced a report dated 30 April 2010 wherein the deficiencies in the rather outdated DPA of 2004 were highlighted in order for Mauritius to introduce the changes required to achieve adequacy with the EU. I quote from the report:

> [the] Mauritian Data Protection Act contains (too) many examples of poor drafting and contradictions. Although inspired from other Acts (e.g. the UK Act), the ideas that were taken up have very often been misunderstood or too broadly interpreted at the time of including them into the Act. As a result, many parts are difficult to understand sometimes even have no sense-or are difficult or even impossible to apply . . .'[3]

The second EU Consultant, appointed by the European Delegation in Mauritius, produced a second EU report dated 9 December 2011 on the amendments to be brought to the DPA in order to align it with international EU data protection principles, and reiterated in her report the observations of the first EU consultant as follows:

> The Commissioner and staff of the DPO are to be commended for operating under rather limited human, office and technological resources.
>
> The creation of several technical guidelines in house of excellent quality, the conduct of investigations and the sheer volume of registrations handled is a credit to the Commissioner and her staff.[4]

The office has received the comments of the European Commission regarding whether the amendments proposed are internationally compliant so that the parent ministry can proceed to the submission of the draft amendment bill to cabinet and then to the national assembly.

Through the amendment made to Section 21 of the DPA in 2009 the functional independence of the Commissioner is since guaranteed, that is,, the Commissioner is not subject to directives from the Prime Minister, although it operates under the 'aegis' of the Prime Minister's Office. The office also submits an annual report to the National Assembly.

It was only by the end of 2010 that an 'investigation unit' was created at the office consisting of three IT experts and investigations thus started based on the visits effected by the officers and the complaints received at the office. The relevant statistics show that up to now, 10 Volumes of Guidelines have been published on different aspects of data protection by the Commissioner, one code of practice for the Mauritius Police Force with regard to the operation of CCTV cameras for road traffic purposes, 14 decisions rendered on complaints received, 18 complaints are currently under investigation, 8,953 data controllers have been registered with the office, 122 site visits including security checks and compliance

3 At p. 106 of the confidential report entitled 'Analysis of the Adequacy of the Protection of Personal Data provided in Mauritius' prepared by the CRID.

4 At p. 75 of the report dated 9 December 2011 titled 'Ensuring the compliance of the Data Protection Legislation and Principles of Mauritius with EU Standards'.

audits have been effected, and 2,720 certificates of registration have been delivered to registered data controllers. All the presentations, publications, training, and workshops produced by the office are also available on our website,[5] which was designed and launched in 2009.

The office has focused a great deal of effort on sensitization campaigns through the media, mainly on television and the press, and has also launched a helpdesk facility together with online facilities for the submission of complaints and registration forms to the office. Recently, a project in collaboration with the Ministry of Education has been prepared by this office with regard to the inclusion of data protection into the primary and secondary curricula in order to teach data protection principles in our schools. A 'teen' corner is also to be found on our website for creating awareness among young people on the dangers associated with making personal information known to the public.

Technical assistance has now been sought from the European Commission for the creation of better tools to improve these sensitization campaigns. Further assistance has also been sought from our Canadian counterpart for the creation of a research laboratory on data protection.

Challenges for the Commissioner's Office

The most challenging task for the Commissioner remains the close supervision of all investigations carried out by the officers, formerly known as investigators and now known as 'Data Protection Officers', and giving reasoned decisions in a timely manner, the latter being a constant reminder for the office of its limited resources to perform this task with huge implications.

The first hurdle is that the Commissioner, who was a state counsel before joining the office, is the only person in the office with a legal background, and all decisions are delivered by her without a quorum, which is not usually the case for other commissions or tribunals. The main reason for this state of affairs is a lack of interest expressed by those in the legal circuit to join the office and the scarcity of those with the required expertise. However, no mention of the requirement for a quorum is made in the DPA, which therefore obligates the Commissioner to give decisions *in solo*.

The second hurdle is that the Commissioner, whilst delivering her decisions which are all based on the facts and peculiarities of each case, despite insufficient resources, attempts to seek inspiration from international jurisprudence, but is also required to apply the provisions of the DPA despite the fact that these provisions were characterized in the CRID Report as being incongruous and confusing. However, the Commissioner does not believe that she should try to apply unclear or ambiguous sections of the law that cannot, in essence, provide a reasonable conclusion. For example, Parts IV and VII of the DPA, which are two of the most important parts, are typical areas of the law which are inflicted with such vagueness, and the first EU Consultant declared in the CRID Report that substantial amendments are required to bring the DPA of 2004 in line with current international principles. Subject to clear rules of admissibility of evidence being introduced by way of an amendment to the current DPA, there is, further, a legal vacuum with regard to whether the general rules followed in criminal cases are sufficient and can be adapted to data protection cases.

In these circumstances, the Commissioner is often left to her own legal intuitions to determine the decision to be given in each case. The virtual impression is indeed comparable to the discovery of an otherwise unknown territory by an adventurer, in a 'Robinson Crusoe' style. It is the belief of the Commissioner that the more challenging the issue is, the more careful she should be in exercising her powers in a harsh way, especially upon those who genuinely were not aware that they may be committing potential offences under the DPA, and only after a very careful scrutiny of the proportionality and seriousness of the impact of the action disputed as compared to the prejudice and/or harm caused to the victim.

Fortunately, in this alien territory, parties can exercise their right of appeal before the Information and Communication Technologies Appeal Tribunal and ultimately the Supreme Court. The right of appeal is always communicated to the parties via a covering letter attached to the decision being despatched to them. The parties have 21 days as from the receipt of the letter to exercise their right of appeal under Section 58 of the DPA. Out of 14 decisions, only one has been appealed and that is currently pending before the ICT Appeal Tribunal. Recent decisions have also shown that when the commission of an offence under the DPA has been clearly proven beyond reasonable doubt by the complainant against the respondent, it is referred to the police for prosecution under Section 20 of the DPA, which then refers the matter to the Director of Public Prosecutions under the normal criminal procedure of Mauritius. Section 63 of the DPA further elaborates on the prosecutorial powers of the Commissioner before the Intermediate Court, which has jurisdiction in data protec-

5 See <http://dataprotection.gov.mu> accessed 1 July 2013.

tion matters, and all prosecutions are instituted subject to the consent of the Director of Public Prosecutions.

All enquiries are completed once the complainant declares to this office that it is satisfied with the enquiry conducted. If the complainant is not satisfied, the enquiry is pursued so that more evidence, wherever possible, is gathered. This in no way precludes the complainant from appealing against the decision of the commissioner once he/she receives it. However, the weight to be attached to the appeal is an issue for the appellate tribunal or court to decide.

The guidelines published by the office are meant to educate the public and do not, in any circumstance, substitute for the binding rules which are the provisions of the Data Protection Act, and the Commissioner explicitly makes reference only to the sections of the DPA in her decisions to avoid any confusion about the interpretation of the legal issues at stake and the ambit of the guidelines. This is not to say that the guidelines contradict the law, but they contain much practical advice and opinion which go beyond the provisions of the DPA and are meant only to be recommendations, and are thus limited to offering assistance on the implementation of its provisions in light of the obvious dearth of jurisprudence at the international level on this subject.

For instance, the guidelines refer to ignorance of the law not being a legitimate excuse for those who want to fraudulently use this defence. But this does not in any way preclude the Commissioner from taking this factor, amongst others, into consideration in order to conclude that no criminal intent was genuinely found and proved beyond reasonable doubt. Furthermore, the decisions of the Commissioner are essentially based on the facts and do not aim to provide unnecessary lengthy analysis of the law in issue but to do so in a very concise way.

Decisions issued by the Commissioner

The Commissioner having been a state prosecutor, she is also able to bear in mind while applying the provisions of the DPA that not all infringements should automatically lead to prosecutions, there being, on one side, the letter of the law and, on another side, the spirit of the law (as per Montesquieu's legal philosophy).

An example where the spirit of the law compels the Commissioner to take into account fairness and the interests of justice was one particular case criticized by the author referred to above.[6] In that case, the Respondent cooperated with the office in returning the CV of the complainant, even though this was not done earlier, and no prejudice was found to have been caused to the complainant through the alleged unjust retention of the CV; thus, the Commissioner decided not to prosecute the respondent for an offence where he obviously did not have any criminal intention.[7] This is not to say that in all cases of unjustified retention of personal information the Commissioner would apply the same principles of non-prosecution, as this will depend on the particular facts and circumstances of the case and the seriousness of the crime involved. Even though the DPA is silent on this aspect, the Commission also has a conciliatory role and reaching settlements to cases is part of its basic function. This is why the subtle interplay between civil and criminal fundamentals is self-evident in its decisions and have to be analysed in a very practical manner to give the case its due merits. It is to be borne in mind that the Mauritian legal system is hybrid as it incorporates both French and English law.

Again referring to the comments made by the author relating to another decision,[8] I quote from the decision: 'An opt-in consent clause system may also be envisaged by Respondent No.1 to confirm express consent of the customers electronically together with the signing of the appropriate consent forms as already catered for by him.' However, the author erroneously interpreted the Commissioner's decision as requiring express consent, which in this particular case logically should be written, as an electronic opt-in consent cannot be oral, it must *always* be written.[9] In fact, oral consent may be accepted as 'express consent', as long as it meets all the evidentiary requirements and suits the particular circumstances of the case. The Commissioner may raise the standard if she finds that written consent is more justified in these circumstances. The fact that the guidelines refer to the possibility of oral consent does not mean that in all cases oral consent would be enough to prove a case beyond reasonable doubt. Additionally, in this case, the respondent was already manually collecting the consent forms, so that there is no harm in respondent doing so electronically. If the Commissioner, from an evidentiary perspective, finds that oral consent needs to be confirmed or supported by other evidence because of a lack of clarity or quality, she has the power to ask for such consent to be written. The Commissioner does not have to explain in the decision itself the distinction to be made between the evidential weight of the consent as contrasted with the

6 See Makulilo (n 1), at 134.

7 Decision No 1 at <http://dataprotection.gov.mu/English/Pages/Decisions-on-Complaints.aspx> accessed 1 July 2013.

8 Decision No 3 at <http://dataprotection.gov.mu/English/Pages/Decisions-on-Complaints.aspx> accessed 1 July 2013.

9 Makulilo (n 1), at 134–7.

admissibility of the consent. The motivation for asking for written consent is based on the facts of the case.

> I also quote from Article 29 Data Protection Working Party opinion 15/2011 on the definition of consent, which guided this decision:
>
> Consent does not have to be recordable to be valid. However, it is in the interest of the data controller to retain evidence. Obviously, the strength of the evidence provided by a specific mechanism may vary, providing more or less evidence of the consent. Consent that has been obtained through a clickable button with the identity of the individual supported with an email address only will have much less evidentiary value than a similar process that is supported, for example with recordable consent mechanisms. The need for strong evidence will also depend on the type of data collected and the purpose followed: an electronic signature will not be needed to consent to receiving commercial offers, but may be necessary to consent to the processing of certain types of financial data on-line. Explicit consent given in an on-line environment will need to be recordable so that it is accessible to be used for subsequent reference.[10]

When the Commissioner makes explicit reference to other laws applicable to the particular set of facts apart from the DPA in her decision, this does not stand to mean that she is applying other factors beyond the provisions of the DPA as the author alluded to in his article.[11] The DPA cannot be applied in isolation from other laws and certainly does not prevail over them, unless expressly provided as, for example, in the DNA Identification Act, where it is stipulated that the Data Protection Act does not apply to this particular processing of personal information.

To quote from a decision of the Commissioner criticized by the author:[12]

> It would seem that if the reasoning of Respondent is applied, all complainants wishing to seize this office for action, have to be, a priori, authorised by management to exercise their rights. Should the management of Respondent not be agreeable, then the person should not lodge a complaint. The Commissioner would like to point out that this particular course of action would be tantamount to a clear breach of the principles enunciated in our constitution, the Data Protection Act and the Employment Rights Act. In this context, the Commissioner is also of the view that complainants have rights embodied under the Data Protection Act which allow them as data subjects whose rights have been violated, to appeal to the Commissioner to recommend corrective measures and/or prosecute those at fault. If a complainant, employee of a particular institution, feels that his privacy rights have been violated during his employment, he may lodge a complaint at this office without fear of being reprimanded or subject to a warning or dismissed because a complaint has been lodged at this office. The right to lodge a complaint cannot be defeated by the fact that the employee has not informed management of the nature of the complaint which is not even directed against the employer and the latter cannot under any circumstance, use a complaint made to this office as a weapon for potential dismissal and for the conduct of disciplinary proceedings on the ground that Complainant has lodged a complaint which is indirectly prejudicial to it being given that the latter has allegedly made a complaint against another colleague who has sent unsolicited emails to other colleagues or people. This is indeed a violation of the sacrosanctity of the right to legal action.

It is clear that this decision makes explicit reference to the principles contained in the Data Protection Act and applies the provisions of the DPA, in particular when it also refers to Section 27 of the DPA for implementation by Respondent of the appropriate security and organizational measures.

There is further no legal restriction in the DPA preventing the Commissioner from disclosing non-personal information in a decision which is not of a confidential nature and which does not involve the parties to the case (that is, the complainant and the respondent) but involve, for instance, business entities which have been involved in the enquiry.

Conclusions

To conclude, I would like to emphasize the multi-facetted roles that the Commissioner and her office are regularly called upon to execute, which include, amongst others, delivery of legal opinions on the relevant sections of the DPA, authorizations for transfers of personal data abroad, and the production of timely guidelines every year. We aim to deliver an efficient service to the nation every day, and will continue to do so even though the challenges are growing day by day. There is indeed always room for improvement and we would certainly not say that we are perfect. But we focus all our efforts on making data protection part of every citizen's daily routine, and we do not forget to remind them, at every available opportunity, that they have a right to be forgotten and a right to be left alone (although not an absolute one), when their personal data are justifiably at stake.

doi:10.1093/idpl/ipt018
Advance Access Publication 8 August 2013

10 Article 29 Working Party, 'Opinion 15/2011 on the definition of consent' (WP 187, 13 July 2011), at 26.

11 See Makulilo, note 1 above, at 131.

12 Decision No 10 on <http://dataprotection.gov.mu/English/Pages/Decisions-on-Complaints.aspx>. See Makulilo, note 1 above, at 138.