

**Cour
Pénale
Internationale**



**International
Criminal
Court**

Original: English

No.: ICC-01/05-01/08

Date: 3 October 2016

TRIAL CHAMBER III

Before: Judge Joyce Aluoch, Presiding Judge
Judge Geoffrey Henderson
Judge Chang-ho Chung

**SITUATION IN THE CENTRAL AFRICAN REPUBLIC
IN THE CASE OF
THE PROSECUTOR
V. JEAN-PIERRE BEMBA GOMBO**

**Public Redacted Document
with**

Confidential, *EX PARTE*, only available to the Prosecution and Registry Annex A

Public redacted version of "Prosecution's Response to the Report of the Registrar pursuant to oral Decision of 12 January 2011", 14 March 2011,

ICC-01/05-01/08-1325-Conf-Exp

Source: The Office of the Prosecutor

Document to be notified in accordance with regulation 31 of the Regulations of the

Court to:

The Office of the Prosecutor

Ms Fatou Bensouda

Mr James Stewart

Mr Jean-Jacques Badibanga

Counsel for the Defence of Jean-Pierre

Bemba Gombo

Mr Peter Haynes

Ms Kate Gibson

Legal Representatives of Victims

Ms Marie-Edith Douzima-Lawson

Legal Representatives of Applicants

Unrepresented Victims

**Unrepresented Applicants for
Participation/Reparation**

**The Office of Public Counsel for
Victims**

Ms Paolina Massidda

**The Office of Public Counsel for the
Defence**

Mr Xavier-Jean Keita

States Representatives

Amicus Curiae

REGISTRY

Registrar

Mr Herman von Hebel

Counsel Support Section

Victims and Witnesses Unit

Mr Nigel Verrill

Detention Section

**Victims Participation and Reparations
Section Other**

I. Introduction

1. On the Court premises, the Office of the Prosecutor (“Prosecution” or “OTP”) disclosed confidential materials to the Defence. Thereafter, without first encrypting the disk or protecting the confidential material with a password, Defence counsel took the disk out of the building, put it in his luggage, and left his luggage unattended on the train to Schiphol Airport. Someone opened counsel’s luggage and stole his encrypted laptop computer and the unencrypted disk.

2. The Registry, conducting an investigation at the request of Trial Chamber III (“Chamber”), concludes that the Prosecution did not comply with Section 27.3 of the Administrative Instruction on the ICC Information Protection Policy ICC/AI/2007/001 (“AI”) and an internal Prosecution regulation, and that noncompliance “may result in disciplinary action [...] [against] the responsible staff member(s). Such behaviour would fall under the definition of ‘unsatisfactory conduct’ under [OTP] Staff Rule 110.1.” It notes, however, that the decision whether to take disciplinary measures lies within the discretion of the Prosecution.

3. The Prosecution submits that the Registry has no authority to analyse the merits of disciplinary sanctions against the Prosecution’s staff in a report to the Chamber, much less to determine that the Prosecution conduct violated internal prosecution regulations and could, in the discretion of the Prosecutor, result in disciplinary action. The outer limits of the Registry’s mandate is to provide the facts to the Chamber – i.e., to inform the Chamber that the Prosecution disclosed material to the Defence on an unencrypted disk that was not password-protected. The Prosecution does not further read the Chamber’s direction to instruct the Registry to assess whether one or more Prosecution staff members violated internal OTP rules or regulations.

4. In accordance with Article 42.2, the staff of the OTP is independent, cannot receive instruction from any other source than the Prosecutor, who has full authority over them. Therefore it is for the Prosecutor to determine whether the acts of OTP staff members violate internal OTP regulations and, if so, whether and to what extent disciplinary proceedings should be initiated. In this instance, the Prosecution appropriately assessed the acts of its staff and concluded that there was no violation of any regulations or other administrative provisions.

5. The Prosecution further notes that its own conclusions are identical to those reached by the Information Security Management Forum (“ISMF”), an inter-organ group (which included three representatives of the Prosecution, the Information Security Officer, and six other representatives of the Registry) that met on 19 January 2011, one week after the Chamber asked the Registry to look into the facts. The 19 January meeting was specifically organized to consider the issues arising from this incident and to discuss how to mitigate the risk of incidents similar to the one described above from happening in the future.

6. The Prosecution expresses its concern that the Registry formulated a judgment inconsistent with its functions.

II. Background

7. On 7 January 2011, the Registrar filed a report in which it informed the Chamber that a member of Jean-Pierre Bemba’s Defence team left his luggage unattended on the train between The Hague and Amsterdam Schiphol; items were removed from his luggage, including his password protected laptop computer and an unencrypted DVD which the Prosecution had provided to the Defence counsel. The DVD contained lightly

redacted documents with details of 17 witnesses scheduled to testify in the case against Jean-Pierre Bemba, including address and location details of some of the witnesses.¹

8. [REDACTED]²

9. On 19 January 2011, an inter-organ group, the ISMF, met specifically and solely to discuss the implications of the lost laptop and disk. The Registry was represented by seven persons, including staff persons from the Victims and Witnesses Unit and the Information Security Officer. The Prosecution was represented by three persons. According to the minutes of the meeting, the Registry's Information Security Officer stated that "disclosure of OTP was not in violation of the relevant [Administrative Instructions] because the (digital) information was treated just as classified information on paper; which is allowed".³

10. On 21 February 2011, the Registry filed the "Report of the Registrar pursuant to oral decision of 12 January 2011" ("Registry Report").⁴ The Report concluded *inter alia*, that "the storage and transmission of [information classified as CONFIDENTIAL or above] in a non-encrypted [form] and without Strong Password did not comply with Section 27.3 of the ICC/AI/2007/001 and Regulation 21 of the OTP Regulations".⁵ It further concluded that "[n]on-compliance with Section 27.3 of ICC/AI/2007/001 may result in disciplinary action under Section 40.3 of ICC/AI/2007/001 [against] the responsible staff member(s). Such behaviour would fall under the definition of 'unsatisfactory conduct' under Staff Rule 110.1", which may result in "disciplinary

¹ ICC-01/05-01/08-1100-Conf, Result of risks assessments related to theft of laptop, 7 January 2011. [REDACTED].

² [REDACTED]

³ See Annex, p. 2.

⁴ ICC-01/05-01/08-1277-Conf, Report of the Registrar pursuant to oral decision of 12 January 2011, 21 February 2011.

⁵ *Ibid*, para. 37.

proceedings against responsible staff member(s) of the OTP”.⁶ It added that “[t]he decision to initiate disciplinary proceedings against responsible staff member(s) of the OTP is under the discretion of the Prosecutor pursuant to Staff Regulation 10.2(a), Staff Rule 110.4(a) and Sections 2.1 and 3.1 of Administrative Instruction ICC/AI/2008/001 (“Disciplinary Procedures”)”.⁷

III. Request for confidentiality

11. The Prosecution requests that this response be received by the Chamber as Confidential, *Ex Parte*, Prosecution and Registry as it cites a transcript from a closed proceeding and internal working group minutes.

IV. Prosecution’s submissions

The Registry overstepped its mandate in reaching conclusions about the OTP’s staff conduct and the merits of OTP disciplinary measures

12. “The Registry shall be responsible for the non-judicial aspects of the administration and servicing of the Court, without prejudice to the functions and powers of the Prosecutor in accordance with article 42.”⁸ As further described in the Rules of Procedure and Evidence, the Registry shall “serve as the channel of communication of the Court”;⁹ be “responsible for the internal security of the Court, in consultation [...]”;¹⁰ “keep a database containing all the particulars of each case [...] and “maintain the other records of the Court”;¹¹ perform functions relating to victims and

⁶ *Ibid*, para. 38.

⁷ *Ibid*, para. 39

⁸ Article 43(1) of the Rome Statute (“Statute”).

⁹ Rule 13(1) of the Rules of procedure and evidence (“Rules”).

¹⁰ Rule 13(2) of the Rules.

¹¹ Rule (15) of the Rules.

witnesses;¹² and provide support and assistance to the Defence.¹³ It also manages the detention facility.¹⁴ And it may assist the Presidency, where appropriate, in the enforcement of fines, forfeiture, and reparation orders.¹⁵

13. As noted previously, the Registry's exercise of its functions cannot be done in a manner that will cause "prejudice to the functions and powers of the Prosecutor". The Prosecutor shall "have full authority over the management and administration of the Office." Further, "A member of the Office shall not seek or act on instructions from any external source".¹⁶ In that regard, the Prosecution submits that the Registry cannot determine that a member of the Prosecution staff would be properly subject to discipline by the Prosecutor. The Registry's overreach is not ameliorated by its acknowledgement that the Prosecutor retains the exclusive discretion to determine whether to bring disciplinary action. To the contrary that acknowledgement is a recognition of its lack of competence to pass judgment on the behaviour of the Office of the Prosecutor staff.

The Registry's conclusion that OTP staff members violated the AI is incorrect

14. The Registry's intrusion into the Prosecutor's authority is aggravated by the substantial error in its conclusions, including that it ignores and contradicts the conclusion reached by its internal expert in security protection.

15. The Information Security Management Forum,¹⁷ made up of three Prosecution and seven Registry representatives, met a week after the Chamber referred the fact-finding matter to the Registry. It concluded that the Prosecution did not violate any

¹² Rules 16-19 of the Rules.

¹³ Rules 20-22 of the Rules.

¹⁴ Regulation 90 of the Regulations of the Court.

¹⁵ Regulation 16 of the Regulations of the Court.

¹⁶ Article 42(2) of the Statute.

¹⁷ The ISMF is an advisory board to the Registrar and the Prosecutor, see ICC-ASP/9/34.4.25.c.

provision by providing *inter partes* disclosure, on Court premises, of confidential materials contained on a disk that was not encrypted or password-protected. As reflected in the minutes of that meeting, the Information Security Officer (a staff member within the Registry) explained that “the disclosure of OTP was not in violation of the relevant [Administrative Instructions] because the (digital) information was treated just as classified information on paper; which is allowed. The information might have been incorrectly labelled however labelling did neither cause nor would have prevented the information loss.”¹⁸ The Information Security Officer has the mandate, pursuant to a Presidential Directive of 2005, to advise the Court and its organs “on risks, opportunities and measures with regard to information security”.¹⁹

16. The Prosecution informs the Chamber that its own internal assessment, reached a similar conclusion. Its analysis, based on an accurate reading of the AI provisions, is set forth below.

17. Section 27.3 of the AI provides that “Information classified [ICC] CONFIDENTIAL and above *may* be stored on Court provided secure USB memory sticks. Information classified [ICC] CONFIDENTIAL and above *may* be stored on other portable storage media such as floppy disks, DVD and CDs if the information on the media is encrypted and accessible only via a Strong Password or functional equivalent” (italics emphasis added).

18. The use of the word “*may*” in Section 27.3 connotes that the storage on secure memory sticks or other encrypted and password protected storage media is not required. Section 27.4 of the AI corroborates that it is not mandatory for the Prosecution

¹⁸ Annex, p. 2.

¹⁹ ICC/PRES/D/G/2005/001, 8 March 2005, Section 3.10 provides that “The Information Security Officer (ISO) has been delegated responsibility for the Court's information security process and shall coordinate and monitor the information security efforts in the Court. In addition, the ISO shall provide to the ICC and its organs advice on risks, opportunities and measures with regard to information security.”

to store confidential information on DVDs in encrypted form and with strong passwords. Section 27.4 applies with respect to “Information classified [ICC] CONFIDENTIAL and above [that] is stored on portable storage media not compliant to the conditions set out in subsection 27.3”. For that information - the information not stored on secure flashdrives or encrypted and password protected storage media - Section 27.4 provides that “the portable storage media shall be regarded equivalent to hard copy versions of the information they contain and inherit the highest classification of the information stored on them, and shall be protected accordingly”. Under the AI, this would include adding appropriate markings to designate the security classification level. Each Confidential document on the disk was, accordingly, appropriately marked. Moreover, the contents of the disk, which can only be seen when the disk is loaded onto a computer, were protected from inadvertent disclosure to others while it was being transported within the building.²⁰

19. As a result of the above, the mere storage of confidential information on a non-encrypted electronic storage media and the handing over of such media to the Defence on the premises of the Court does not constitute any violation of the AI. Otherwise, transporting non-secure electronic copies or hard copies of confidential information to and from the courtroom, but always within the premises of the ICC building, would equally constitute a violation of the AI.

20. Moreover, Section 27.4 of the AI must be read in conjunction with Sections 30 and 31, which regulate the manner in which confidential information may be transported within the premises of the Court or outside as well as within and between ICC premises. Section 30, which addresses the carrying of classified materials within the premises of the Court, provides:

²⁰ See, e.g., AI, Section 30.1.

30.1 Documents classified CONFIDENTIAL and above that [are] carried within the Court premises (including any field office) shall be covered in order to prevent observation of [their] contents.

30.2 Documents classified CONFIDENTIAL and above shall, when removed from secure storage, at all times be under surveillance by a Staff.

Section 31 addresses the removal of material from the Court premises and imposes additional security obligations. It provides:

31.1 Information shall be removed from the Court premises only when there is a reasonable expectation that the Information will be protected in compliance with or equivalent to the provisions of this A.I.

31.2 Information classified RESTRICTED and above shall be removed from the Court premises only when required for the conduct of official use.

31.3 Information classified CONFIDENTIAL and above shall be under constant surveillance by Staff and kept in a cover sheet.


21. In particular, Section 31 applies to information in hard copy as well as information stored on DVDs or CDs in non-encrypted form and without strong password protection pursuant to Section 27.4 of the AI, and requires that any such transfer is conducted in a manner that protects the information.

22. In short, the Prosecutor informs the Chamber that after analyzing the acts of the OTP's staff, he concluded that there was no violation of any regulations or other administrative provisions.

V. Conclusion

23. For the reasons stated above, the Prosecution requests that the Chamber (a) take note of the fact that the Prosecution disclosed confidential materials to the Defence via

an unencrypted DVD that was not password-protected, to be used in the Premises of the Court, and (b) dismiss the Registry's comments regarding the Prosecution's alleged failure to comply with the relevant AI.



Fatou Bensouda, Prosecutor

Dated this 3rd Day of October 2016
At The Hague, The Netherlands