Translated from French

UNITED NATIONS DISPUTE TRIBUNAL	Case No.:	UNDT/GVA/2010/049 (UNAT 1682)
	Judgment No.:	UNDT/2011/056
	Date:	23 March 2011
		English
	Original:	French

Before: Judge Jean-François Cousin

Registry: Geneva

Registrar: Víctor Rodríguez

DERICHE

v.

SECRETARY-GENERAL
OF THE UNITED NATIONS

JUDGMENT

Counsel for Applicant:
Anne-Marie Demmer

Counsel for Respondent:
Shelly Pitterman, UNHCR

Introduction

1. By application filed with the secretariat of the former United Nations Administrative Tribunal on 31 March 2009, the Applicant contests the decision dated 20 July 2007 whereby the United Nations High Commissioner for Refugees ("High Commissioner") imposed a written censure on him together with the loss of two steps in grade.

2. The Applicant seeks the annulment of the abovementioned disciplinary sanctions, together with compensation for the material and moral damage suffered as a result of the said sanctions.

3. The case, which was pending before the former UN Administrative Tribunal, was transferred to the United Nations Dispute Tribunal on 1 January 2010 pursuant to the transitional measures set forth in General Assembly resolution 63/253.

Facts

4. The Applicant entered the service of the Office of the United Nations High Commissioner for Refugees ("UNHCR") on 1 September 1988 on a fixed-term appointment that was extended several times. In 1995, he was given an indefinite appointment, and, at the date of the impugned actions, he had served since 1 November 2004 as Senior Desk Officer, level P-4, in what was then the Bureau for Central and South-West Asia, North Africa and the Middle East ("CASWANAME") in Geneva.

5. On Friday 1 September 2006, at 11.51 a.m., the email account of the Head of the North Africa Desk of CASWANAME, who was at the time the Applicant's supervisor, was accessed using the Webmail interface, which enables UNHCR staff members to consult their email accounts via the Internet.

6. On the same day, at 1.19 p.m., an anonymous email was sent from the address "fairhonnest2006@yahoo.com" to the Inspector General's Office at

UNHCR ("IGO") as well as to several senior officials, including the Deputy High Commissioner, the Controller, the Spokesperson, the Directors of the Division of Human Resources Management ("DHRM"), the Division of Operational Services and the Division of International Protection Services, and the Heads of the Bureau for Africa and the Bureau for the Americas. Attached to that email as a PDF document was another email sent on 31 August 2006 by the Head of the North Africa Desk to the representative of a government, thanking him "for the jewelry [he] had sent [her]". The text of the anonymous email stated that the attached document showed that a senior UNHCR official was receiving gifts from a government, pointing out that the government in question was a party to a conflict and that the region in which that conflict was taking place fell within the responsibilities of the Head of the North Africa Desk, and it called for "urgent action from UNHCR management".

7. The Applicant, who had also received a blind copy of the email sent from the address "fairhonnest2006@yahoo.com", forwarded it to the Director of CASWANAME a few hours later.

8. After receiving the abovementioned email, IGO opened an investigation into the allegations that the Head of the North Africa Desk had accepted gifts in breach of staff regulation 1.2 in force at the time. In the course of the investigation, the Head of the North Africa Desk admitted that she had in fact received jewelry from a government representative and that she had thanked him in the email of 31 August 2006. It was also confirmed that the jewelry was of low value and that she had given it to a colleague the same evening.

9. At the end of that first investigation, IGO opened another investigation into the unauthorised access to the email account of the Head of the North Africa Desk. A number of interviews took place as part of this investigation, including with the Applicant and the Head of the North Africa Desk. On 12 September 2006, when asked by IGO, the Head of the North Africa Desk stated that she had given the password to her email account to her secretary, the Applicant and the

UNHCR Telecoms Unit and that she had not logged in to her email account via the Webmail interface on 1 September 2006.

10. On 29 September 2006, IGO sent the Applicant a draft report of the preliminary investigation which showed that at the time the email account of the Head of the North Africa Desk had been accessed via the Webmail interface, 11.51 a.m on 1 September 2006, three people were using that software, whose computers were identified by their respective IP addresses, and one of them was the Applicant's. It also showed that at 11.55 a.m. on 1 September 2006, the printer assigned by default to the Applicant's computer had been used and that at 11.59 a.m., a Google search had been made from the Applicant's computer of the first and last names of the government representative to whom the email of 31 August 2006 had been sent. It showed, too, that the message sent anonymously on 1 September 2006 from the address "fairhonnest2006@yahoo.com" came from the Applicant's computer, as did the document in PDF format attached to that email. Lastly, it stated that, when asked what he had been doing between 11.50 a.m. and 1.19 p.m. on 1 September 2006, the Applicant had given no explanation, but that records had revealed that at 1.28 p.m. he had taken the lift from the garage to the UNHCR offices.

11. On 5 October 2006, the Applicant submitted his observations on the draft preliminary investigation report, claiming that he had nothing to do with the sending of the email on 1 September 2006.

12. IGO submitted the final version of its preliminary investigation report on 9 October 2006 and sent it to the Director, DHRM. The report stated that the evidence justified the conclusion that the Applicant had accessed the email account of the Head of the North Africa Desk without authorisation, that he had copied the email of 31 August 2006 and then sent it to several senior officials under cover of an anonymous email.

13. On 20 October 2006, the Director, DHRM personally handed the Applicant a letter dated 11 October 2006 together with the IGO report. The letter set out the acts he was alleged to have committed, namely that he had accessed

another staff member's Webmail account without authorisation in order to obtain a copy of an email, and sent it in the form of a PDF document to a number of senior managers. She stated that, if the facts were established, they would constitute misconduct within the meaning of staff rule 110.1 and invited him, pursuant to administrative instruction ST/AI/371, to submit his observations in response to those allegations.

14. The Applicant submitted his observations on 17 November 2006, reiterating his denials, and claiming that at lunchtime on 1 September 2006 he had gone shopping to buy something for a dinner to which he had been invited that evening.

15. On 9 January 2007, the Director, DHRM informed the Applicant that she intended to submit the case to the Geneva Joint Disciplinary Committee ("JDC") and had decided to suspend him with full pay for an initial period of two months, which was later extended. On 26 January 2007, the case was referred to the JDC, which forwarded a copy of the file to the Applicant on 7 February 2007. In the course of its review the JDC carried out a site visit in spring 2007, making the journey between the Applicant's office and the shop where he claimed to have made purchases on 1 September 2006.

16. In its report dated 13 July 2007, the JDC considered that the facts alleged were established, and that they constituted misconduct within the meaning of staff rule 110.1 as the Applicant's actions contravened, among other things, the Secretary-General's bulletin ST/SGB/2004/15 entitled "Use of information and communication technology resources and data", and memorandum No. IOM/FOM/54/2005 on the IGO role and functions. Consequently, it recommended that the High Commissioner apply a written censure to the Applicant, together with the loss of two steps in grade.

17. The High Commissioner forwarded the report of the JDC to the Applicant under cover of a letter of 20 July 2007, and decided to accept its findings and recommendations.

18. On 31 March 2009, having obtained six extensions of time, the Applicant filed an application with the former UN Administrative Tribunal appealing against the Secretary-General's decision. On 28 September 2009, having requested and been granted two extensions of time by the UN Administrative Tribunal, the Respondent filed his answer. The Applicant, who was granted two extensions of time, submitted observations on 31 December 2009.

19. On 1 February 2010, having obtained two extensions of time, the Applicant filed an amended version of his observations with the Dispute Tribunal. The Respondent filed comments on the said observations on 29 March 2010.

20. By letter of 10 February 2011, the Registry of the Dispute Tribunal notified the parties of the decision of the Judge assigned to the case to hold a hearing.

21. On 9 March 2011, the hearing was held in the presence of the Applicant, his Counsel, and Counsel for the Respondent.

Parties' contentions

22. The Applicant's contentions are:

a. The IGO preliminary investigation was not conducted with thoroughness and objectivity. The fact that the High Commissioner took no account of the lacunae in the investigation breaches the Applicant's right to due process as well as the principle of the presumption of innocence;

b. The inferences drawn by the JDC are neither reasonable nor sufficiently founded. By contrast to the method applied by the JDC to the taking of evidence, it is not for the Applicant to prove his innocence and his initial inability to recall what he was doing on 1 September 2006 at the time the events took place should not count against him. Nor should the fact that he did not speculate about the identity of the third party who allegedly used his computer to carry out the acts imputed to him;

c. The JDC was wrong to reject the Applicant's explanations regarding his absence from his office, and to place greater reliance on its site visit even though that did not enable it to faithfully reconstruct the facts;

d. The JDC did not accept the hypothesis that a third party could have committed the facts held against the Applicant, while photos taken by him in October 2008 showed that it was perfectly possible for someone to have sat at his workstation and then used the printer without being noticed, on 1 September 2006 between 11.50 a.m. and 1.30 p.m., especially in view of the fact that the colleague with whom he shared his office was absent that day. Staff members at UNHCR can access the network from any workstation, and, furthermore, persons who are not necessarily UNHCR staff members have free access to the building at lunchtime to eat in the cafeteria. The fact that three emails were opened in the Applicant's professional email account at the time when the disputed facts were taking place does not prove that he was present at the time. Nor does the fact that the online course on harassment he was following was not closed until the end of the afternoon. Lastly, the acts he is alleged to have committed seem irrational for someone of his experience, and would have required a particular motive. But the motive imputed to him by the JDC for committing the said acts, the tension that allegedly existed between him and the Head of the North Africa Desk, lacks credibility, as she told the JDC that she thought their relations were good until the events in question occurred. There is, in addition, a contradiction between, on the one hand, taking account of his past loyalty and team spirit as mitigating circumstances and, on the other, accepting the existence of tensions in the workplace as a motive for the acts alleged;

e. The evidence gathered in the course of the investigation is incomplete, questionable, and insufficient to establish that the Applicant committed misconduct: (i) the Administration has not produced the file containing a list of logins to the network. As his computer was not

connected to a scanner, such a list would enable the exact time he turned on his computer to be verified, as well as whether he logged in from another workstation connected to a scanner; (ii) while it is established that the Applicant did use the Webmail interface at 11.51 a.m. on 1 September 2006, there is nothing to prove that he accessed the email account of the Head of the North Africa Desk. The investigation should have identified all the persons who were already using the interface and who could have logged in to that email account; (iii) the file used as the basis of the preliminary investigation report was not the original file attached to the email sent from the address "fairhonnest2006@yahoo.com", but a file that had been renamed and perhaps altered, which had been saved in a shared folder and did not show the properties of the original; (iv) the computer on which the file attached to the email sent from the address "fairhonnest2006@yahoo.com" had been created has not been identified. Therefore, the finding in the preliminary investigation report that the Applicant had created that file is erroneous; (v) if the Applicant had logged into the network from a workstation other than his own in order to use a scanner, two IP addresses would have been given for the same period, one for each machine being used; (vi) it is not possible to determine, from the log file of the print server, either the properties or the name of the document the Applicant produced on the default printer assigned to his computer. The Applicant could perfectly well have created a document in PDF format from his computer and an examination of the hard drive of his computer would have revealed whether the attachment to the email of 1 September 2006 came from it; (vii) the Applicant's old workstation was replaced by a new computer while he was serving his suspension, and the Administration failed to preserve it. It has therefore not been inspected, despite a number of requests by the Applicant; (viii) there is nothing to indicate that IGO attempted to trace the identity of the person who had set up the "fairhonnest2006@yahoo.com" address through the Yahoo server, and the Applicant's attempts to do so have been unsuccessful; (ix) there is nothing, either, to indicate that IGO entertained the hypothesis that another

person logged in to the email account for the "fairhonnest2006@yahoo.com" address, and it has not been established that it was the Applicant who accessed it; (x) the particular configuration of his computer could give the impression that the Applicant himself had logged in to his professional email account, when in fact he had not; (xi) IGO did not take action to obtain the recordings of the surveillance cameras posted at the entrances to the building, though the investigation had established that the Applicant had entered the UNHCR building via the garage and taken the lift at 1.28 p.m.;

f. At the time the events took place, there was no procedure governing the use of passwords. Despite the loopholes in the electronic security system at UNHCR, neither IGO nor the JDC considered the hypothesis that the password of the Head of the North Africa Desk had been misused by someone else.

23. The Respondent's contentions are:

a. The Secretary-General had a broad scope of discretion in disciplinary matters under staff regulation 10.2 and Chapter X of the Staff Rules in force at the time. The Under-Secretary-General for Management, on behalf of the Secretary-General, delegated his disciplinary authority to the High Commissioner, who duly exercised it;

b. The facts held against the Applicant are established. He accessed the email account of the Head of the North Africa Desk without her authorisation. The JDC considered whether another person might have used his workstation to send the email on 1 September 2006, but it took the view that such a hypothesis was highly unlikely as it implied that the third party in question must have known both the Applicant's password and that of the Head of the North Africa Desk, and taken a great risk in spending one and a half hours at the Applicant's workstation to search, on Google, the first and last names of the government representative to whom the email of 31 August 2006 had been sent, as well as searching the terms

"accountability", "IGO" and "IOMFOM/2005/iom5405.htm" on the UNHCR intranet. The theory that the Applicant's computer was being used remotely, for instance by a hacker, was considered but ruled out in the end because it would have required someone at the Applicant's workstation to accept the remote access. It also presupposed a particular motive, which was lacking in the present case. The Applicant retrieved an email from the email account of the Head of the North Africa Desk, without authorisation. The Applicant then sent that email, under cover of an anonymous email;

c. The facts held against the Applicant constitute misconduct. Unauthorised access to electronic resources and email accounts and their use in a manner contrary to the rights and obligations of staff members contravenes the provisions of the Secretary-General's bulletin ST/SGB/2004/15 and memorandum No. IOM/FOM/58/2006, which deals with UNHCR policy on electronic mail. The Applicant did not stop at alerting IGO, but sent the message to a number of senior managers. Given the potential consequences of such actions for the Head of the North Africa Desk even before an investigation was held, the Applicant cannot claim to have acted in good faith;

d. The investigation was conducted by IGO in accordance with the provisions of memorandum No. IOM/FOM/54/2005 on the IGO role and functions. The disciplinary proceedings were properly conducted and the rights of the Applicant respected;

e. The sanction imposed is proportionate to the misconduct.

Consideration

24. In contesting the decision dated 20 July 2007 whereby the High Commissioner imposed on him a written censure together with the loss of two steps in grade, the Applicant merely maintains that he did not commit the actions with which he is charged and which are as follows: first, that he accessed his

supervisor's email account without authorisation, second that he made a copy of an email in it, and then that he forwarded it to a number of senior UNHCR officials under cover of an anonymous email.

25. Both in his written submissions and at the hearing, the Applicant has alleged that there were several lacunae in the investigation of the facts mentioned above. He maintained, among other things, that IGO should have examined the recordings of the video surveillance cameras at UNHCR and ensured that the hard disk of his computer was preserved in order to examine it. Even assuming the investigation could have been conducted in a more exhaustive manner, that fact alone does not enable the Applicant to establish that he did not take the impugned actions. The Tribunal must, therefore, base its findings only on those facts that are beyond dispute. The only facts set forth below are those the Tribunal considers are established by the evidence on the record for the day of 1 September 2006:

- At 11.51 a.m., the Applicant's computer, the IP address of which is 10.9.143.44, was connected to the Webmail interface, as were two other computers at UNHCR headquarters;

- At 11.51 a.m., the email account of the Head of the North Africa Desk was accessed via the Webmail interface;

- At 11.55 a.m., one page was printed on the printer assigned as the default printer to the Applicant's computer;

- Between 11.56 a.m. and 11.57 a.m., three emails were opened in the Applicant's work email account;

- At 11.59 a.m., a Google search of the first and last names of the representative of the government to whom the email of 31 August 2006 was addressed was made from the Applicant's computer;

- At 12.03 p.m., one email was opened in the Applicant's work email account;

- A 12.33 p.m., a search was made from the Applicant's computer under the words "accountability", "IGO" and "IOMFOM/2005/iom5405.htm" on the UNHCR intranet;

- At 1.18 p.m., the Applicant's computer connected to the Yahoo website;

- At 1.19 p.m., the Applicant's computer disconnected from the Yahoo website.

26. Therefore, even though uncertainty remains about some of the other operations carried out from the Applicant's computer, the Tribunal has no doubt that the consultation of the email account of the Applicant's supervisor was carried out from his computer, and that all the other steps leading to the sending of an anonymous email to a number of senior UNHCR managers were also taken from that computer.

27. The written pleadings and the discussions at the hearing also show that the Applicant does not dispute that his work computer was used to carry out the operations described above in paragraph 25, but he states that he was not the person who did so, as he was out of his office at the time they were being carried out, namely between 11.51 a.m. at the latest and 1.19 p.m. at the earliest. The Tribunal must therefore now examine whether the hypothesis of intervention by a third person can be taken seriously.

28. In order to maintain that the acts alleged against him were committed by a third party, the Applicant claims that his computer could have been used without his knowledge, because, given the specific way it was configured, and in particular because of the absence of a screen saver, it remained open when it was not in use, and thus no password was required to access it. Since that technical issue was not checked at the time of the investigation by the Inspector General's Office, the Applicant's statements in this regard should be treated as *prima facie* plausible.

29. First, the Applicant contemplates the hypothesis that someone could have logged in to his computer remotely to carry out the wrongful operations. As

became clear during the investigation, such a hypothesis must on any reasonable view be rejected. Aside from the high level of technical competence required, the person in question would have had to know the email password of the Applicant's supervisor, who stated that it was known only to her secretary, the Applicant and the UNHCR Telecoms Unit, and someone would have had to be physically present in front of the Applicant's workstation to accept the request for remote access.

30. Then, the Applicant contends that a third party could have used his computer on 1 September 2006 by entering his office during his absence and using his computer from 11.51 a.m. to 1.19 p.m. If, as the Applicant maintains, the fact that he had not installed a screen saver with a password meant that a third party entering his office could use his computer without his knowledge, the objection referred to above, that such third party would also have had to know his supervisor's password, is equally valid here. In addition, a person acting in such a way would be running a very great risk of discovery.

31. Even allowing for the fact that, at the time and on the date the acts were committed, there were very few staff members in the neighbouring offices, the supposed third party would have had to stay for 88 minutes using the Applicant's computer, with the risk, first of all, that he might come back into his office at any moment, added to the possibility that another staff member would come into the office and discover them. Even assuming the Applicant's statement to be true, that using other people's computers is fairly widespread at UNHCR, it seems certain that the acts committed at that time would inevitably lead to an internal investigation and that the third party ran a very great risk that someone would remember having seen them using the Applicant's computer. The Tribunal considers that, given the risks the supposed third party was running, that person, wanting to injure both the Applicant and his supervisor, would have limited his or her presence in front of the computer in question strictly to the time necessary to perform the operations needed to direct suspicions towards the Applicant, a matter of a few minutes, and would not have stayed in his office for 88 minutes. It thus

appears to the Tribunal that the hypothesis that another staff member committed the acts in question cannot reasonably be entertained.

32. Having ruled out the hypotheses of intervention by a third party, it remains for the Tribunal to examine whether, in spite of what has been said above, there were circumstances making it physically impossible for the Applicant to have committed the said actions.

33. The Applicant maintained, first, that it was impossible for him to open his supervisor's email account, as he did not know the password. His supervisor, however, has contradicted that statement, explaining that she had given it to him and one other person in April 2006, so that they could access her email inbox in her absence, and that she had not changed it since giving it to him. There is no reason to doubt the statements made by the applicant's supervisor.

34. The Applicant then maintained that it would have been impossible for him to be in his office at 1.19 p.m., the time of the last connection to which this case relates. It seems plausible to the Tribunal that the Applicant, who was questioned as part of the investigation two weeks after the events took place, might not have remembered what he was doing during the disputed period. Later, he stated that he had left the UNHCR building on that day to do some shopping, then returned via the garage to put his purchases in his car and took the lift at 1.28 p.m., which, he claims, makes it impossible for him to have been in his office at 1.19 p.m. That said, while it is common ground that he used the lift at the time stated, there is nothing to show that the Applicant had actually been shopping beforehand, and he thus had the time, as the JDC verified during its site visit, to go to the garage between 1.19 and 1.28 p.m. for a quite different reason than dropping off shopping in his car.

35. There is, therefore, no fact or circumstance that would have made it impossible for the Applicant to commit the acts with which he is charged.

36. Lastly, the Applicant maintains that he had no motive to commit the acts with which he is charged. The Tribunal takes the view that, since the

circumstances of the case have removed any reasonable doubt as to the identity of the person committing those acts, there is no need for it to examine whether a motive existed.

37. Since the Applicant has disputed only that he committed the acts with which he is charged, there is no need for the Tribunal to examine whether or not those acts amount to misconduct or whether the sanctions imposed are proportionate.

Conclusion

38. In view of the foregoing, the Tribunal DECIDES:

The application is dismissed.

(*Signed*)

Judge Jean-François Cousin

Dated this 23rd day of March 2011

Entered in the Register on this 23rd day of March 2011

(*Signed*)

Víctor Rodríguez, Registrar, Geneva