REPUBLIC OF SOUTH AFRICA
IN THE HIGH COURT OF SOUTH AFRICA
GAUTENG LOCAL DIVISION, JOHANNESBURG

CASE NUMBER: 26728/2019

REPORTABLE: YES
OF INTEREST TO OTHER JUDGES: YES
REVISED.
21/1/2021

In the matter between:

NOZUKO MANI **APPLICANT**

And

THE INFORMATION OFFICER MINTEK **FIRST RESPONDENT**
MINTEK **SECOND RESPONDENT**

JUDGMENT

WINDELL, J:

INTRODUCTION

[1] This is an application wherein the applicant seeks information from the respondents in terms of the Promotion of Access to Information Act 2 of 2000 ("PAIA"). The applicant seeks the access to the information in order to protect her rights to dignity. The respondents oppose the relief sought on the basis that the

second respondent ("Mintek"), which is a public body, does not have the information sought (section 23 of PAIA). The applicant maintains that the information does exist.

BACKGROUND FACTS

[2] On 24 October 2018, the applicant was appointed at Mintek, into the position of Head: Market Intelligence, with effect from 1 November 2018. On 25 October 2018, the applicant was made aware of an email circulated within Mintek, from a certain Tshepo Mokgatle, addressed to the then Acting Chief Executive Officer, Mr Simelane, Ms Nyanda (the first respondent, hereinafter referred to as "the information officer"), and a certain Mr Mc Kenzie. In the widely circulated email, allegations were made of fraud and impropriety in the interview process that led to the applicant's appointment to the position. The email also alleged a romantic relationship between herself and her immediate supervisor. The contents of the email are defamatory in nature and was clearly intended to impugn the applicant's character and infringes on her right to dignity.

[3] As there is no person employed by Mintek by the name of Tshepo Mokgatle, the applicant through her attorney, wrote a letter to Mintek on 6 November 2018 wherein she sought an undertaking from Mintek to allow her to conduct an independent forensic investigation, at her own costs, into the source and origin of the email. She, *inter alia*, requested access to all the laptops and computers of all the recipients of the email and *"other people identified by the investigators and all and/or any other tools including but not limited to exchange servers that the investigators deem appropriate and necessary to carry out the investigation*." The applicant did not receive the requested undertaking from Mintek. On 5 December 2018, she sent a further email wherein she sought the intervention of Mintek's Board of Directors to commission an independent forensic investigation into the origin and source of the email. Mintek responded on 11 December 2018. In its response it was suggested to the applicant that she first make use of the internal processes through Mintek's "Grievance Procedure".

[4] On 14 January 2019, the applicant lodged a grievance against Mintek. In the letter of grievance the applicant stated the following:

> *"SOLUTION DESIRED*

"Employer to allow me an independent investigation by my experts into the source and origin of the email sent by Tshepo Mokgatle by gaining access into the employer's server and laptops of the executives who received the email, and such access to take place under the supervision of the employer's IT personnel and/or experts in order to protect the integrity and security of the employer's information"

[5] Mintek's "Grievance Procedure" has three stages. After the completion of the first and second stages of the grievance process, Mintek granted the applicant access to the mail server, but not to the laptops. The applicant was not satisfied with the outcome and she referred the matter to the third stage of the grievance process on 29 February 2019. The third stage was chaired by an external person, Ms Singh. During this process the applicant further clarified the nature of her request. She sought the following outcomes:

1. Access to the mail server for the three recipient executives (backup to be restored if required) as this will enable the applicant to determine the source and origin of the contentious email, as well as where and when the contentious email was created; and,

2. The three recipient executives' laptops, for the same purpose as aforesaid.

[6] Ms Singh took into consideration that Mintek has offered the applicant access to the mail server (where according to Mintek, all emails "reside" and individual laptops contain only "mirrored mailboxes"), but that the applicant did not take up Mintek's offer and had not attempted to conduct a forensic analysis on the mail server. The applicant, instead, *"insisted on having blanket access to both the mail server and the recipient executives' laptops."* Ms Singh further took into consideration Mintek's status as a National Key Point[1], and its concerns over preserving the confidentiality and secrecy of its information, and found that, in the absence of any terms of and/or a detailed explanation as to why access to both the laptops and mail server were necessary for tracing the source and origin of the contentious email, it was unreasonable for the applicant to insist on having access to the laptops.

[1] The National Key Points Act 102 of 1980 provides for the declaration and protection of sites of national strategic importance.

[7] The applicant, unsatisfied with the outcome of Ms Singh's finding, conducted her own investigations regarding the origins of the email using the email header and found that the email was created internally by someone within the respondent using Mintek's Internal IT Infrastructure. The local Internet Protocol ("IP") address of the computer or laptop that sent the email was: 10.0.0156. Subsequent to the findings of her investigations she lodged an appeal against the outcomes of the grievance processes to the General Manager within her division. In the appeal she informed Mintek that she had conducted her own investigation which revealed the information referred to above, and that she therefore requested Mintek to provide her with the identity of the person who was using the computer or laptop with IP Address: [....] on 24 October 2018 when the email was sent and all the LOGS for the IP Address: [....] retrieved from the Active Directory (under Domain: [....]) for the dates 19 October 20128 to 25 October 2018 (including 20 October 2018 and 21 October 2018).

[8] The appeal was dismissed on the basis that that there was no sufficient reason to give the applicant access to the executive laptops before she had not exhausted the initial access granted to the mail server. The appeal was dismissed without having regard to the additional information obtained by the applicant.

[9] On 29 April 2019 the applicant submitted a request to access to information in terms of section 18(1) of PAIA and Mintek's PAIA manual. In this regard the applicant requested the following:

> 1. Mintek to provide the applicant with the identity of the employee who was using the IP address: [....] on 24 October 2018 when the email was sent.
>
> 2. All the LOGS for the IP address: 10.0.0.0.156 retrieved from the Active Directory (under domain: [....]) for the dates 19 October 2018 to 25 October 2018 (including 20 October 2018 and 21 October 2018).

[10] The request for information was sent to the information officer in terms of Mintek's PAIA manual. The respondents did not acknowledge receipt of the request nor did it respond to the request. The information was not provided and on 7 June 2019, after the lapse of a 30 day period, the applicant lodged an internal appeal by way of an email in terms of Mintek's PAIA manual against the information officer's refusal to grant access. Despite the fact that the appeal was received by the

respondents, it was, seemingly, ignored. The applicant thereafter instituted the current application on 30 July 2019.

PAIA

[11] Section 25(1) of PAIA states that the information officer to whom the request is made or transferred, must, as soon as reasonably possible, but in any event within 30 days, after the request is received, (a) make a decision in accordance with PAIA whether to grant the request; and (b) notify the requester of the decision. If the request for access is refused, the notice in terms of subsection (1)(b) must, *inter alia*, "*state adequate reasons for the refusal, including the provisions of the Act relied upon".*[2]

[12] Section 27 of PAIA states that if an information officer fails to give the decision, on a request for access to the requester concerned within the period contemplated in section 25(1) of PAIA, the information officer is, for the purposes of this Act, regarded as having refused the request. In terms of section 74(1)(a) of PAIA a requester may lodge an internal appeal against a decision of the information officer of a public body to refuse a request for access. Section 78 of PAIA provides that a requester or third party referred to in section 74 of PAIA, may only apply to a court for appropriate relief after that requester or third party has exhausted the internal appeal procedure against a decision of the information officer of a public body provided for in section 74 of PAIA.

[13] In terms of section 82 of PAIA, the court may grant any order that is *"just and equitable*", including an order in the following terms:

> *"82 (a) confirming, amending or setting aside the decision which is the subject of the application concerned;*
> *(b) requiring from the information officer or relevant authority of a public body or the head of a private body to take such action or to refrain from taking such action as the court considers necessary within a period mentioned in the order;*
> *(c) granting an interdict, interim or specific relief, a declaratory order or compensation;*

[2] Section 25 (3)(a)

(d) as to costs; or

(e) condoning non-compliance with the 180 day period within which to bring an application, where the interests of justice so require."

[14] The information officer did not provide the information to the applicant and in accordance with section 27 of PAIA it is deemed to have been refused. The applicant lodged an appeal against the refusal to provide the information and when she received no response she approached the court for relief. The first issue that therefore needs to be determined is if the applicant exhausted the internal procedures as contemplated in section 74 of PAIA, before approaching the court.

Exhausting of internal remedies

[15] PAIA does not prescribe a procedure for when the appeal is deemed to have been refused as it does in circumstances where the information officer did not provide the information sought.

[16] Section 77(3)(a) of PAIA states that the relevant authority must decide on the internal appeal as soon as reasonably possible, but in any event within 30 days after the internal appeal is received by the information officer of the body. Section 77(7) of PAIA further provides that if the relevant authority fails to give notice of the decision on an internal appeal to the appellant within the period contemplated in subsection (3), that authority is, for the purposes of PAIA, regarded as having dismissed the internal appeal.

[17] The respondents did not give notice of the decision and it is regarded as having dismissed the internal appeal. The applicant has therefore exhausted all internal remedies as contemplated in section 74 of PAIA and was entitled to approach the court for appropriate relief.

Defence in terms of section 23

[18] The respondents do not dispute that the email was created within the environment of Mintek and that Mintek's tools were used when the email was created. It opposes the application on the basis that it does not have in its possession the information sought by the applicant. It relies on section 23 of PAIA. This section states as follows:

“23 Records that cannot be found or do not exist.

(1) If-

(a) all reasonable steps have been taken to find a record requested; and

(b) there are reasonable grounds for believing that the record-

(i) is in the public body's possession but cannot be found; or

(ii) does not exist,

the information officer of a public body must, by way of affidavit or affirmation, notify the requester that it is not possible to give access to that record.

(2) The affidavit or affirmation referred to in subsection (1) must give a full account of all steps taken to find the record in question or to determine whether the record exists, as the case may be, including all communications with every person who conducted the search on behalf of the information officer.

(3) For the purposes of this Act, the notice in terms of subsection (1) is to be regarded as a decision to refuse a request for access to the record.

(4) If, after notice is given in terms of subsection (1), the record in question is found, the requester concerned must be given access to the record unless access is refused on a ground for refusal contemplated in Chapter 4 of this Part.”

[19] It is common cause that the respondents did not comply with section 23 of PAIA. It did not file an affidavit, nor did it attempt to set out the steps taken to find the information sought in the applicant’s request. The respondents, for the first time in these proceedings, aver that the information sought by the applicant does not exist.

[20] In order to explain why Mintek does not have the information, the information officer deposed to the answering affidavit and gave a description of Mintek's system for assigning IP addresses to persons who log on to its mail server: Mintek uses a server that assigns dynamic IP addresses to the electronic devices that log onto the Mintek computer network. A dynamic IP address is a temporary IP address that is assigned at random to users of a network. Whenever a person logs onto the network, the host server automatically assigns an IP address to the device the person is using from a pool of available IP addresses. When that person logs off, the IP address becomes available again to be assigned to another person that logs on. If the first person logs on again, that person would be assigned a different IP address

from the pool. In other words, a dynamic IP is not associated with a particular device that is used to log onto a network. A particular IP address could be assigned to any user logged onto the network at a particular time. Mintek knows the list of IP addresses that make up its pool of dynamic IP addresses, so it is able to tell whether a specific IP address belongs to the Mintek network or not. Mintek is also able to identify the current assigned IP addresses, but Mintek does not keep a record of historical assignments of IP addresses to hardware seeking to log in to its mail servers. Mintek explains that it is impractical to do so due to the sheer volume of assignments per day. As such, Mintek does not have the information at its disposal.

[21] The respondents belatedly filed a confirmatory affidavit by Hendrik Venter ("Venter"), in his capacity as Head of Information Technology Services at Mintek, in which he confirmed that Mintek's mail server assigns dynamic IP addresses, as described above and that Mintek has not kept a record of the "LOGS" or assignments on the dates indicated by the applicant.

[22] The applicant in reply to the respondents' answer submitted that as the information sought is IT related, which is a specialised field, any person alleging that the information is not available must have accessed and interrogated the server. Only a person with IT related qualifications or requisite skills in the IT industry would be able to attest about the operations of the dynamic server. It was contended that the deponent to the answering affidavit does not have the necessary qualifications, experience or skill to speak to IT related matters. It is further submitted that to simply state that the information is not available is not sufficient. The deponent had to explain how she searched for the information, what happened to the information and whether she verified from the server that the information is not available. It is contended that the information officer's evidence is therefore not of any assistance to the court.

[23] The applicant denies that Mintek does not keep historical information and argues that such an allegation is contrary to Mintek's ICT Policy. During argument the applicant referred the court to Mintek's Information and Communications Technology Policy "ICT policy", and in particular clause 15 thereof. Clause 15 states that each user shall be allocated an individual username and password. The allocation of the username and password is done by the information officer through

its officials. For that reason, so it is argued, the respondents are able to identify the official responsible for the subject email. Clause 15 also states that the owner of a particular username will be held responsible for all actions performed using that username. Clause 24 of the ICT Policy furthermore specifically states that Mintek has back up processes and the retention period of data on tape is five years. It is contended that Mintek can therefore still extract information or a report from the Active Directory which shows all individual IP addresses from which a user account was authenticated. The IP address could have been used by a different user but never at the same time. Where the data has been removed from the server or if the logs have been overwritten, historical data can be retrieved through the back up restoration tapes for the dates in question.

[24] Section 81(3) of PAIA states that the burden of establishing that *"the refusal of a request for access complies with the provisions of this Act"* rests on the party claiming that it so complies. The respondents therefore bear the *onus* to convince the court that: (1) all reasonable steps have been taken to find the record requested, and (2) that there are reasonable grounds for believing that the record cannot be found or does not exist. The section is mandatory and stipulates that the respondents must give a full account of all steps taken to find the record in question or to determine whether the record exists, as the case may be, including all communications with every person who conducted the search on behalf of the information officer. Although it is accepted that the use of the word "*believing*" in section 23 of PAIA imposes a lighter burden of proof on the applicant than a term such as "satisfy", the applicant must nevertheless place facts before the court on which the court can conclude that there is reason to believe that the record cannot be found or does not exist[3].

Did the respondents discharge the onus?

[25] The respondents contended that it is unfortunate that the applicant has launched this application when she has had an opportunity to access Mintek's servers for the purposes of her investigation and *"had the applicant taken up Mintek's invitation to*

[3] *Lecuona v Property Emporium CC* 2010 JDR 0417 (GSJ). See also *Vumba Intertrade CC v Geometric Intertrade CC* 2001 (2) SA 1068 (W) at 1071E-H and *FirstRand Bank Ltd v Pather* 2005 (4) SA 429 (N) at 432C-E.

examine its server, the applicant may have been able to confirm independently that Mintek does not keep records of the information requested in this application."

[26] One of the objects of PAIA is to avoid litigation rather than propagate it[4]. The information officer does not explain to the court why she did not respond to both the applicant's application in terms of PAIA and the appeal thereof. The applicant is confronted, for the first time in these proceedings, with an allegation that Mintek does not have the information sought in its possession. It is not clear why this response was not provided to the applicant when she made the application in terms of both the Grievance Procedure and PAIA. The fact that the applicant has been invited to examine Mintek's server does not excuse the respondents from providing the information sought in terms of PAIA. It is important to point out that the information now sought by the applicant was not the information that formed the subject of her initial grievance. Throughout the initial stages of the grievance, the applicant insisted on receiving access to the laptops of the three persons that received the email. In the applicant's request in terms of PAIA she sought the identity of the employee who was using the IP address: [....] on 24 October 2018 when the email was sent and all the LOGS for the IP address: 10.0.0.0.156 retrieved from the Active Directory (under domain: [....]) for the dates 19 October 2018 to 25 October 2018 (including 20 October 2018 and 21 October 2018). It is not the failure of the applicant to inspect the server that resulted in this application but rather the respondents' failure to provide the information. It is unfortunate that the respondents decided to ignore the applicant's request and disregard the aims of PAIA which has now resulted in this application.

[27] The information officer must take all reasonable steps to find the records requested and must file an affidavit setting out a full account of all the steps taken to find the records in question or to determine whether the records exist, including all communication with every person who conducted the search on behalf of the information officer. The answering affidavit of the information officer as well as the confirmatory affidavit by Venter contains only generalised allegations about Mintek's IT processes. The information officer does not inform the court how she searched for the information and what steps she took to obtain and/or to verify the existence or

---

[4] *Claase v Information officer, South African Airways Pty Ltd* (39/06) [2006] ZASCA 134; [2006] SCA 163 (RSA) (30 November 2006) at para [8].

otherwise of that information. The respondents further failed to attach any document or policy of Mintek that is consistent with the allegations made in the answering affidavits. The respondents further failed to set out any account of the steps that were taken to find the record in question, which must include all communications with every person who conducted the search on behalf of the information officer.

[28] In *Quartermark Investments (Pty) Ltd v Mkhwanazi and Another*[5], the Supreme Court of Appeal emphasized the principle that affidavits in motion proceedings fulfil the dual role of pleadings and evidence and that *"they serve to define not only the issues between the parties but also to place the essential evidence before the court."* They must therefore contain the factual averments that are sufficient to support the cause of action or defence sought to be made out. In *Die Dros (Pty) Ltd and Another v Telefon Beverages CC and Others*[6], Van Reenen J expanded on the difference between primary and secondary facts. He explained as follows:

> *"[28] .....Primary facts are those capable of being used for the drawing of inferences as to the existence or non-existence of other facts. Such further facts, in relation to primary facts, are called secondary facts. (See Willcox and Others v Commissioner for Inland Revenue 1960 (4) SA 599 (A) at 602A; Reynolds NO v Mecklenberg (Pty) Ltd 1996 (1) SA 75 (W) at 78I.) Secondary facts, in the absence of the primary facts on which they are based, are nothing more than a deponent's own conclusions (see Radebe and Others v Eastern Transvaal Development Board 1988 (2) SA 785 (A) at 793C - E) and accordingly do not constitute evidential material capable of supporting a cause of action."*

[29] The respondents baldly stated that they conducted their own investigation but failed to provide any evidence of any investigation they allege to have conducted. If regard is had to the averments that the respondents made in their answering affidavits, there is a total absence of primary facts setting out the steps that were taken to find the information sought by the applicant. If a public body wants to rely successfully on the defence in section 23 of PAIA, it is not sufficient to make

---

[5] 2014 (3) SA 96 (SCA).
[6] 2003 (4) SA 207 (C)

generalised allegations regarding the IT processes. Sufficient and detailed information is required. The averments set out in the answering affidavit are hopelessly inadequate and does not provide any assistance to a court in deciding whether there are reasonable grounds for believing that the record cannot be found or does not exist. The respondents have failed to discharge the *onus* of showing, on a balance of probabilities, that the record does not exist or that it cannot be found.

CONCLUSION

[30] In an application of this nature the applicant has to state what the right is that she wishes to exercise or protect. The applicant must also state what information is required and how that information would assist her in exercising or protecting her right. The right that the applicant seeks to protect is the right to dignity. The information sought is the identity of the employee who was using Mintek's laptop or computer with a specific IP address and all the LOGS for the IP address.

[31] The respondents failed to comply with the provisions of section 23 of PAIA and failed to discharge the onus to establish that the record does not exist. However, for the court to give a final order and order access would not be appropriate before the respondents have not complied with the provisions of section 23 of PAIA. In the result, the following order is made:-

1. A *Rule Nisi* is hereby issued returnable on 5 March 2021 calling upon the respondents to show cause, if any, why the following orders, should not be made final:
   1.1 The first and second respondents are ordered to provide the applicant with the identity of the employee who was using the second respondent's computer or laptop with IP Address: [....] on 24 October 2018 when the email was sent.
   1.2 The first and second respondents are ordered to provide the applicant with all the LOGS for the IP Address: [....] retrieved from the Active Directory (under Domain: [....]) for the dates 19 October 2018 to 25 October 2018 (including 20 October 2018 and 21 October 2018).

2. The respondents are granted leave to file a supplementary affidavit or affidavits in compliance with the provisions of section 23 of PAIA on or before 12 February 2021.
3. The applicant is granted leave, on receipt of the respondents' supplementary affidavit or affidavits, to file a supplementary replying affidavit on or before 26 February 2021.
4. The costs of the application to be paid by the respondents on the scale as between attorney and client.

L. WINDELL

JUDGE OF THE HIGH COURT OF SOUTH AFRICA

GAUTENG LOCAL DIVISION, JOHANNESBURG

Delivered: This judgement was prepared and authored by the Judge whose name is reflected and is handed down electronically by circulation to the Parties/their legal representatives by email and by uploading it to the electronic file of this matter on CaseLines. The date for hand-down is deemed to be 22 January 2021.

APPEARANCES

Counsel for applicant:	Adv M. Gwala SC
Attorneys for applicant:	Ngeno & Mteto Inc.
Counsel for respondent:	Adv. S. Swartz
Attorneys for respondent:	Webber Wentzel Attorneys
Date of hearing:	8 September 2020
	(Additional heads of argument were submitted by
	the applicant and the respondents on 7 December

2020 and 3 December 2020 respectively).

Date of judgment: 22 January 2021