

REGULATORY

The Consequences of Lessons not Learnt – A Cautionary POPIA Tale

27 August 20256 min read

by Dakalo Singo, Director & Head of Pro Bono and Ahmore Burger-Smidt, Director & Head of Regulatory

"All men make mistakes, but a good man yields when he knows his course is wrong, and repairs the evil. The only crime is pride." — Sophocles

In a disturbing case of history repeating itself, the South African Police Service (SAPS) has once again allowed private personal information – information that they are entrusted with and obliged to protect and keep confidential – to circulate and appear publicly on WhatsApp groups and other social media platforms. This *repeat offence* is highlighted in the recent urgent application of ***KM v Minister of Police and Others*** [2025] ZANCHC 53.

Mr KM was the sole eyewitness in a case involving the murder of his employer. He made statements to the SAPS regarding the crime, doing so with the belief that his personal information would be kept private and confidential. However, he subsequently discovered that a confidential internal SAPS communication, containing his name and the address where the crime occurred (which is his address), had been leaked when he saw the communication circulating on WhatsApp and other social media platforms. Mr KM argued that he was utterly shocked and traumatised by the disclosure of his personal information. He also argued that he now lives in fear for his life and personal safety.

One could question whether Mr KM's concerns are legitimate and/or justified, or whether his application was brought merely to derive compensatory benefits. However, history presents numerous examples of individuals who have suffered harm – including intimidation, threats, and even death – following a data breach or disclosure of their personal information.

Internationally, for example, the Centre for Free Expression has detailed how whistleblowers often become targets of intense reprisals, such as targeted violence, death threats, and even assassination: *"It's not unusual for whistleblowers to receive death threats."*^[1] In a further example, a Human Rights Watch report details the account of a survivor of domestic violence in Turkey, where the police revealed the location of the shelter, at which she was hiding, to her abusive husband, leading to a violent confrontation and further abuse.^[2] In another example, following a data breach by police and other organisations in the United Kingdom (also affecting survivors of domestic violence), the UK's Information Commissioner remarked that *"These families reached out for help to escape unimaginable violence, to protect them from harm and to seek support to move forward from dangerous situations. But the very people that they trusted to help, exposed them to further risk"*, with the Domestic Abuse Commissioner for England and Wales adding that *"For victims of domestic abuse, a data breach can be a matter of life or death"*.^[3]

Considering these examples, it is evident that the risks and dangers faced by the witness to a horrific crime are equally grave. It is difficult to understand how the SAPS allowed such a disclosure to occur, especially when policies, processes, and security measures should exist to safeguard the personal information entrusted to them.

The unfortunate reality is that the circumstances faced by Mr KM are not an isolated incident. In July 2022, the survivors of a highly publicised criminal attack in West Village, Krugersdorp were similarly shocked to learn that an internal SAPS communication containing their personal information – including their names, residential addresses, occupations, and the number of men that had raped them during the attack – had been leaked on WhatsApp and other social media platforms.

Following the Krugersdorp personal information leak, the [Information Regulator issued an Enforcement Notice against the SAPS](#) in April 2023, in which it found that the SAPS had breached various provisions of POPIA by leaking the personal information of the survivors. The Information Regulator held, amongst things, that the SAPS had failed to comply with the conditions for the lawful processing of personal information (i.e. lawfully and in a reasonable manner that does not infringe their right to privacy). It was further held that the SAPS failed: to establish and maintain appropriate safeguards; to regularly verify the safeguards; and to ensure updates in response to new risks being identified with specific reference to WhatsApp. Additionally, the Information Regulator ordered, amongst other things, that the SAPS take measures to ensure that such an incident or any incident of a similar nature does not recur.

Given the circumstances in Mr KM's case, it appears that the measures taken by the SAPS, if any, are self-evidently inadequate. Instead of *"repairing the evil"*, as Sophocles encourages, the SAPS have allowed a repetition of the same evil.

Mr KM's application was ultimately dismissed. While the court recognised that the SAPS *"failed in their duty to serve and protect the applicant"*, it held that it was unable to grant Mr KM the *"extraordinary relief"* that he had argued for.

It is worth noting, however, that in his application, Mr KM neither refers to, nor relies on POPIA. Despite his application being unsuccessful, the SAPS' conduct effectively exposed the SAPS' failure to adhere to POPIA. In terms of POPIA, it remains within Mr KM's rights to refer a complaint to the Information Regulator against the SAPS, alleging interference with the protection of his personal information. Additionally, Mr KM may also, in terms of POPIA, institute a civil claim for damages against the SAPS.

It is disconcerting that the SAPS has failed to learn the lessons that it should have learnt from its previous breach of POPIA (in the Krugersdorp matter). This is made worse by the fact that the breaches concerned are not merely a nuisance to the affected people but actually place them in real and potentially mortal danger. One such breach was already excessive; but the SAPS' repeated conduct now highlights a larger institutional disregard for the right to privacy.

But unlike Sophocles' above view that *"the only crime is pride"*, the SAPS' shortcomings in this respect constitute a multitudinous array of rights violations.

Ultimately, when a lesson is not learnt, an injustice stands to be repeated.

[1] <https://cfe.torontomu.ca/guidesadvice/whistleblowers-ordeal> (accessed on 8 August 2025).

[2] <https://www.hrw.org/report/2011/05/04/he-loves-you-he-beats-you/family-violence-turkey-and-access-protection> (accessed on 8 August 2025).

[3] <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/09/data-breaches-put-domestic-abuse-victims-lives-at-risk-uk-information-commissioner-warns/> (accessed on 8 August 2025).



Ahmore Burger-Smidt

Head of Regulatory

[View Profile](#)



Dakalo Singo

Head of Pro Bono

[View Profile](#)