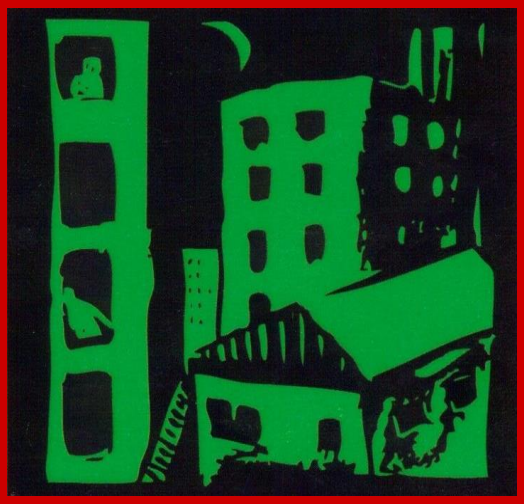
LAW
DEMOCRACY
& DEVELOPMENT



VOLUME 28 (2024)

DOI: http://dx.doi.org/10.17159/2077-4907/2024/ldd.v28.3

ISSN: 2077-4907

The prevalence of cybercrimes and hacking incidents and their impact on the confidentiality of documents in civil proceedings

NOMBULELO QUEEN MABEKA

Associate Professor, Department of Jurisprudence, University of South Africa, Pretoria, South Africa

https://orcid.org/0000-0003-3627-0523

ABSTRACT

Confidentiality is important in legal practice as it obligates legal practitioners to protect clients' information. It is often linked to the right to privacy entrenched in section 14 of the Constitution of the Republic of South Africa, 1996. The link is made on the basis of clients' entitlement to attorney-client confidentiality. Furthermore, the rules of courts in civil proceedings require legal practitioners to include clients' personal or confidential information in court documents, including their identity numbers. The requirement of clients' personal information in court documents is found in particular in Rule 3(A)(1)(b)(i) of the Uniform Rules of Court, 2009 as amended. This personal information is uploaded online in the CaseLines system, as required by Practice Direction 1 of 2023, a situation which poses a

significant risk because such information may be hacked and used to commit cybercrimes. Current legislation, such as the Protection of Personal Information Act 4 of 2013, seeks to provide guidelines on how courts should protect confidential information which is included in the pleadings or affidavits. The Practice Directives, however, are silent on measures that should be taken to protect confidential information. Item 18 of the E-Rules and the Draft Amended Magistrates' Courts Rules seek to protect confidential information to a certain extent, but these have not yet been implemented. The article examines current legislation, the respective rules of court, and the approach followed by the courts, in order to determine whether confidentiality does indeed exist in civil proceedings. In addition, it briefly compares the online civil proceedings of South Africa and the United Kingdom to ascertain their differences and similarities.

Keywords: confidentiality; personal information; POPI Act; Rule 3A & Rule 35; Item 18 of the E-Rules; Draft Amended Magistrates' Courts Rules; South African Practice Directives; Practice Direction 31 of the United Kingdom.

1 INTRODUCTION

In civil procedure, a matter is brought before a court by either action or application proceedings.[1] In application proceedings, the application is brought by notice of motion supported by founding affidavits. The notice of motion explains the prayer that the applicant seeks, and the affidavits provide personal information of the applicants in civil procedure matters.[2] The applicants are required to disclose their qualifications and identity numbers in the affidavits.[3] For example, Rule 3A of the Uniform Rules of Court of 2009 provides that applications for admission of advocates must disclose qualifications and identity numbers, and this application is unopposed.[4] If any other matter is opposed in application proceedings, the respondent must file an answering affidavit which contains confidential information such as identity numbers.[5]

It may be argued that qualifications fall within the ambit of personal information in terms of section 1(1) of the Protection of Personal Information Act 4 of 2013 (the POPI Act).[6] The same applies to information relating to identity as required for the admission of advocates in terms of Rule 3A of the Uniform Rules of Court, as well as to an affidavit that incorporates the identity number of the practitioner who applied to be admitted as an advocate.[7] It is contended here that the current civil proceedings processes hinder

[1] Broodryk T *Eckard's principles of civil procedure in the Magistrates' Courts* (6th ed) Cape Town: Juta (2019) at 44; Theophilopoulos C, van Heerden CM, Boraine A & Rowan A *Fundamental principles of civil procedure* (4th ed) Durban: LexisNexis (2020) at 157–170.

[2] *Replication Technology Group and Others v Gallo Africa Limited and Others* 2009 (5) SA 531 (GSJ) para 19.

[3] Rule 35 of the Uniform Rules of Court, 2009 and Rule 23 of the Magistrates' Court Rules, 2010.

[4] Section 26 of the Legal Practice Act 28 of 2014; Rule 3A of the Uniform Rules of Court, 2009.

[5] Theophilopoulos et al. (2020) at 167.

[6] Section 1 of the Protection of Personal Information Act 4 of 2013 (POPI Act) .

[7] Rule 3A(1)(b)(i) of the Uniform Rules of Court.

the protection of personal information afforded by section 14 of the Constitution. The stipulations of the POPI Act give effect to the constitutional right to privacy, yet application proceeding matters still disclose the applicants and respondents' personal information.

While cognizance is taken of the fact that the parties to civil proceedings consent to the disclosure of their personal information, it is averred that this is a major risk, especially when the notice of motion that is filed electronically includes founding affidavits.[8] The risk lies in the possibility that hackers or unlawful interceptors may hack the application proceeding papers, which include the notice of motion, together with affidavits, since these contain personal information about the parties and may be used to commit cybercrimes such as cyberfraud. A classic example is taking the identity numbers that appear on the notice of motion and affidavits and which are uploaded on the CaseLines system[9] and using them to open fictitious bank accounts for the purposes of money laundering.

Against the backdrop above, this article analyses the statutes in South Africa that protect personal information. It also examines the rules that compel the parties to civil proceedings to include personal information, such as identity numbers, in the affidavits annexed to the notice of motion. Finally, the article assesses whether the current civil processes do in fact protect personal information.

2 THE DISTINCTION BETWEEN CONFIDENTIALITY AND PRIVACY

Before examining the relevant statutes that regulate privacy, it is necessary to distinguish between confidentiality and privacy. It is important to mention first that the concept of "confidentiality" originates from the common law. In *Helen Suzman Foundation v Judicial Service Commission,*[10] the Constitutional Court held that confidentiality is significant in legal proceedings and that the nature of the information determines the level of protection that should be afforded.[11] The Court in *Genesis One Lighting v Jamison and Others*[12] defined "confidential information" as "that which is not in the public domain or public knowledge". Strom and Earhart define "confidentiality" as a "duty that prevents certain people from sharing information with third parties".[13]

[8] Items 18 and 50 of Directive 2 of 2022.

[9] Item 50 of Directive 2 of 2022.

[10] *Helen Suzman Foundation v Judicial Service Commission* 2018 (4) SA 1 (CC).

[11] *Helen Suzman Foundation* (2018) at para 63.

[12] *Genesis One Lighting v Jamieson and Others* (19/3212) 2019 ZAGP JHC 93 (18 March 2019).

[13] Strom S and Earhart R "Is there a difference between confidentiality and privacy?" (2024) available at https://www.findlaw.com/criminal/rights/is-there-a-difference-between-confidentiality-and-privacy.html (accessed 8 January 2024).

Legal practitioners have this duty in respect of their clients' information, which they must keep confidential.[14]

Insofar as "privacy" is concerned, Strom and Earhart assert that "generally, an action is private if you have a reasonable expectation of privacy while doing the action".[15] They argue further that privacy is breached when private information is disclosed. Recently, the Constitutional Court, in *Arena Holdings Pty Ltd t/a Financial Mail and Others v South African Revenue Services and Others,*[16] confirmed that section 14 of the Constitution protects privacy. It is therefore prudent to analyse the stipulations of section 14 of the Constitution.

3 RELEVANT STATUTES REGULATING CONFIDENTIALITY OR PERSONAL INFORMATION

3.1 The Constitution of the Republic of South Africa

Section 14 of the Constitution guarantees the protection of the right to privacy. *Bernstein v Bester,*[17] a long-standing authority on the protection of the right to privacy, was decided under the Interim Constitution Act 200 of 1993. This case demonstrated the strict approach which the Constitutional Court follows in matters regarding the infringement of the right to privacy. The courts have a duty to protect the right to privacy; equally, the legislature views the protection of the right as significant. It is, however, important to remember that the right to privacy is not an absolute right because it is subject to the limitation clause test provided for in section 36 of the Constitution. Section 36 stipulates the factors to be considered when seeking to balance conflicting rights. The courts have performed this balancing act in a multitude of cases over the years.[18]

A case in point is South *African Airways Soc v BDFM Publishers (Pty) Ltd*.[19] *In casu,* the Court limited the right to confidentiality because it was in the public's interest to do so. Currie and De Waal concur with the Constitutional Court. They opine that this right deserves to be preserved at all costs and that it may be limited only in terms of section 36 of the Constitution.[20] When applying section 36, it must be borne in mind that the law of civil procedure permits the disclosure of parties' personal information in some court papers. Such information is confidential, however, and, as mentioned, the situation poses a risk to parties. In the light of these considerations, it is thus submitted that it is opportune to review the obligation to disclose confidential or personal

[14] *All G2 G Ltd and Others v van Rensburg and Others* (59644/2020) [2021] ZAGPPHC 425.

[15] Strom and Earhart (2024).

[16] *Arena Holdings Pty Ltd t/a Financial Mail and Others v South African Revenue and Others* 2023 (5) SA 319 (CC) 13 at para 80.

[17] *Bernstein v Bester* 1996 (2) SA 751 (CC).

[18] *Tshabalala-Msimang v Makhanya &Others* 2008 (6) SA 102 (W) at para 43.

[19] *South African Airways Soc v BDFM Publishers (Pty) Ltd* 2016 (1) All SSA 860 (GJ) at paras 61–65.

[20] Currie I & de Waal J *The bill of rights handbook* (6th ed) Cape Town: Juta (2014) at 295.

information, which may expose parties to the risk of falling victim to cybercrimes.[21] The question this article raises is: To circumvent cybercrime, is it not time to review the obligation to disclose confidential or personal information in affidavits such as identity numbers?

This consideration is all the more important given that Practice Directive 1 of 2023 enforces the use of the online CaseLines system in civil proceedings. The Directive requires parties to the proceedings to upload confidential information on the CaseLines system.[22] In addition, the E-Rules: Draft Amended Uniform Rules introduce an e-justice system that will operate online when these rules become effective.[23] The rules will apply despite the fact that cybercriminals could unlawfully intercept any information which is uploaded electronically unless stringent measures are in place to guard against hacking or unlawful interception.[24] In the absence of safety measures, criminals may hack the online court system through phishing or spoofing.[25] This could occur when the registrar creates a file online through CaseLines and invites parties to the proceedings to upload their court documents.[26] There is thus a court website that may be susceptible to spoofing.[27] Hackers could steal confidential information through phishing and spoofing attacks. Van der Merwe contends that information may be obtained through phishing and that this may be accomplished by sending an email to parties to request that they update their electronic details.[28] Van der Merwe further states that phishing appears to be the "most sophisticated" method of unlawfully obtaining clients' information.[29]

It may be argued, then, that online civil proceedings pose a major risk to the parties concerned and that proceedings implicitly expose them to the risk of becoming victims of cybercrime. Consequently, if courts and legal practitioners do not introduce appropriate measures to protect clients' confidential information, they may be the cause of their falling prey to cybercrime. As such, it is important to analyse the relevant

---

21 Theophilopoulos et al. (2020) at 351–359, 514.

22 Practice Directive 1 of 2023.

23 Item 1A of the E-Rules: Draft Amended Uniform Rules.

24 Snail S "Cybercrimes in South Africa – Hacking, cracking, and other unlawful online activities" (2009) 1 *Journal of Information, Law & Technology* at 4–5.

25 Lenaert-Bergmans B "Understanding the differences between spoofing vs phishing" (2023) available at https://www.crowdstrike.com/cybersecurity-101/attack-types/spoofing-vs-phishing/ (accessed 9 January 2024).

26 Practice Directive 2023.

27 The Judiciary of South Africa available at https://www.courtonline.judiciary.org.za (accessed 11 January 2024).

28 Van der Merwe D "Criminal law" in Van der Merwe D et al. *Information and communications technology law* (3rd ed) Durban: LexisNexis (2021) at 80.

29 Van der Merwe et al. (2021) at 80.

legislation that gives effect to the protection afforded in terms of the constitutional right to privacy.

3.2 The POPI Act

The POPI Act was passed to give effect to the right to privacy as provided in section 14 of the Constitution. The provision in the POPI Act which is pertinent in protecting confidential information is found in section 1(b) and (c). These clauses concern:

> (b) information relating to the *education* or the *medical*, financial, criminal or employment history of the person;
> (c) any identifying number, symbol, e-mail address, *physical address*, telephone number, location information, online identifier or other particular assignment to the person …[30]

In interpreting this provision, it is important to highlight that the meaning of personal information includes identity numbers, as illustrated in subsection (b). This is usually the case in practitioners' admission applications, as provided in Rule 3A(1)(b)(i) of the Uniform Rules of Court. Section 1(b), which relates to information pertaining to education, medical and financial position, is also important because if, for example, the cause of action in a case arises out of a disclosure of medical records – as was the case in *NM v Smith*[31] and *Tshabalala-Msimang v Makhanya* – this must be pleaded. This implies that the plaintiff or defendant's medical or financial personal information must be included in the pleadings to show the cause of action. If this is not done, the claim may be deemed as defective. The question is: Does the consent to the disclosure provided in section 11 of the POPI Act justify the contravention of section 1 of the POPI Act?

Some practitioners are required to obtain clients' identity numbers, which must be included in the founding affidavit. It is argued that hackers may intercept the clients' educational information and commit identity theft, as Cassim indicates.[32] Further, the identity numbers of clients, which are included in the founding affidavits and admission applications, may be used to commit cybercrimes if this information is hacked by cybercriminals by spoofing and phishing the CaseLines system and online court system governed by Practice Directive 1 of 2023, as well as by spoofing and phishing the e-justice system regulated by the E-Rules: Draft Amended Uniform Rules. The website for online court processes may be attacked by hackers through spoofing or phishing in order to obtain personal information contained in the court documents uploaded on the CaseLines system or Court Online system.[33] This is different to the physical process of accessing files in the respective courts because there is a register or a record kept by the court, one which incorporates details of those who request the inspection of the file.

---

[30] Emphases added.

[31] *NM v Smith* 2007 (5) SA 250 (CC).

[32] Cassim F "Addressing the growing spectre of cybercrime in Africa: Evaluating measures adopted by South Africa and other regional role players" (2011) *The Comparative and International Law Journal of Southern Africa* 123 at 138.

[33] The judiciary available https://www.courtonline.org.za (accessed 11 January 2024).

Cognizance is taken of the fact that the client information uploaded on the court electronic system is contained in public documents. However, in any form of electronic communication there is a risk of unlawful interception. If clients' identity numbers are used to commit cybercrimes, the consequences may be dire for such clients, and their reputations stand to be tainted. As Roos argues:

> personal data must, in terms of this principle, be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measure …[34]

Some legal practitioners and court officials argue that court papers are viewed as public-domain information and do not require the courts to enforce additional measures to protect personal information filed electronically in accordance with the CaseLines system.[35] It is contended, however, that a review of the process is necessary and that there is a need to amend the rules which require that clients' identity numbers be used in founding affidavits and admissions applications, as indicated in rule 3A(1)(b)(i) of the Uniform Rules of Court. In the light of the privacy risks which parties to civil proceedings face, the possibility exists of legal action against the registrar of the court in executing his or her duties. Rule 3A requires the applicants to file documents that include the identity number of the applicant. The question arises as to who would be liable for the damages that such an applicant may suffer as a result of such unlawful interception. This is a matter of concern that calls for consideration of the modification of the current rules to protect the personal information of legal practitioners' clients.

There are authors who assert that Practice Directive 1 of 2020 is silent on the protection of personal information in the application of Rule 35 of the Uniform Rules of Court and Rule 23 of the Magistrates' Court Rules.[36] It is also observed that Directive 2 of 2022 is equally silent on the protection of personal information in civil proceedings.[37] It is for this reason that it is argued here that an amendment of the current rules and directives is needed so as to provide for stringent measures to protect personal information contained in online court processes or systems. In doing so, the courts would also be enforcing section 42 of the Regulation of Interception of Communications and Provisions of Communication-Related Information Act 70 of 2002 (RICA).

---

[34] Roos A "Data privacy law" in Van der Merwe D et al. (3rd ed) *Information and communications technology law* Durban: LexisNexis (2021) at 417.

[35] Batchelor B "Online litigation- preparing for the new normal" (2023) 1 *De Rebus* at 6–7; Mabeka NQ "An analysis of the implementation of the CaseLines System in South African Courts in the light of the provisions of section 27 of the Electronic Communications and Transactions Act 25 of 2002: A beautiful dream to come true" (2021) 1 *Potchefstroom Electronic Law Journal* at 11.

[36] Mabeka NQ "An analysis of the implementation of the CaseLines System in South African Courts in the light of the provisions of section 27 of the Electronic Communications and Transactions Act 25 of 2002: A beautiful dream to come true" (2021) 1 *Potchefstroom Electronic Law Journal* at 17.

[37] Practice Directive 1 of 2020.

In addition, the rules that compel the parties to the proceedings to include their physical addresses in court papers pose a major risk to the plaintiff or the defendant. The physical address is included in the definition in subsection 1(c) of the POPI Act. This is a worrying fact, particularly in cases of civil claims that arise from damages suffered as a result of cyberfraud. Cybercriminals may hack the CaseLines system (which is in an electronic communications format) and obtain the physical address in order to intimidate the applicant in opposed matters. They may do this to force the applicant to withdraw the civil claim in matters that involve high-profile people.

This is said notwithstanding the fact that court papers are public documents and can be inspected physically. The physical inspection does offer protection of the information to a certain extent because the details of those who inspect the files are recorded in a register maintained by the court. By contrast, online hacking is difficult to control, manage, and track because hackers hide their identities and sometimes are never found. The inspection of the court file is different because there is a record kept that is completed by those who go to the court to view the files. The record incorporates the details of those who inspect the court files, and they can be easily tracked, whereas in the case of online hacking, not everyone can track the hackers. Item 18 of the E-Rules seeks to protect confidential documents to a certain extent. This rule states:

> (18)*(a)* The confidentiality of an electronic record or a document therein shall be dealt with the same as for the equivalent paper record. *The electronic filing system may permit access to confidential information only to the extent provided by law*. *No person in possession of a confidential electronic record, or an electronic or paper copy thereof, may release the information to any other person except as provided by law.*[38]
>
> (b) If a registered user seeks court approval to seal a document, the registered user may file the document electronically under temporary seal pending court approval of the registered user's motion to seal …

It is submitted that the consent given by the plaintiffs and defendants is not enough in the light of the rapidly evolving nature of cybercrime. Hackers (needless to say) do not ask permission to access confidential information, and utilise dubious means to bypass online safeguards. It must be noted that the rule above does not offer any practical guidance as to how information may be reasonably protected against hackers.

In *South African Airways Soc v BDFM Publishers (Pty) Ltd*,[39] the Court interpreted the meaning of "confidential information" in the context of the principle of privilege. It was argued that the information was obtained in confidence and given to one in the capacity of a legal advisor.[40] It was asserted that the information in question that was claimed to be confidential was contained in the founding affidavit.[41] The Court concluded that information shared between legal advisors and their clients is subject to the limitation clause in section 36 of the Constitution. It also held that the right may be limited on the

[38] Emphasis added.

[39] *South African Airways Soc v BDFM Publishers Pty Ltd and Others* 2016 (1) All SA 860 (GJ).

[40] *South African Airways* (2016) at para 6.

[41] *South African Airways (*2016) at para 13.

grounds of public interest.[42] The Court held that "once confidentiality is shattered, like Humpty Dumpty, it cannot be put back together again".[43] It further stated that "any relief sought from a court to protect any form of confidential information is subject to any recognised public interest overrides, an exercise which requires a balancing of contending values in a fact-specific context …"[44]

It is observed that the Constitutional Court followed a strict approach in determining whether there was an infringement of confidentiality in information shared between the client and the legal practitioner. Roos argues that "only personal data, that is data that relate to a person and permit identification of a person, is affected".[45] This view is supported here, particularly insofar as the application of Rule 18 of the E-Rules and Draft Amended Magistrates' Court Rules is concerned. It is common cause that founding affidavits include the identification of a person, as Roos indicates. It is important to highlight the fact that Item 18 of the Draft Amended Magistrates' Courts Rules is similar to Item 18 of the E-Rules. In fact, the two items are verbatim replicas of each other, and therefore the argument that applies to the E-Rules is also applicable to the Draft Amended Magistrates' Courts Rules. Consequently, reference to Item 18 encompasses both rules.

Furthermore, with respect to Roos's averment that the personal information affected is not regarded as private, it may be argued that this personal information, particularly in civil proceedings, deserves specific protection that the courts should enforce. This argument is bolstered by Dreyer, who states: "Computer technology has not created new methods of invading the privacy of individuals. It has merely made it easier because of the speed at which the ease with which information about individuals can be manipulated and transmitted …"

It must be pointed out that the sealing of the information in terms of Rule 18 justifies the argument submitted above. Snail and Papadopoulos argue that clients in practice should have an option to decide whether or not confidential information should be used in civil proceedings.[46] They affirm that the right to privacy enjoyed protection by common law long before its entrenchment in section 14 of the Constitution. The authors further affirm their support for the disclosure of confidential information when it is in the public interest, as was upheld in the *South African Airways* case.[47] Snail and Papadopoulos also assert that:

---

[42] *South African Airways (*2016) at paras 61–65.

[43] *South African Airways (*2016) at para 38.

[44] *South African Airways (*2016) at paras 53–54.

[45] Van Der Merwe (2021) at 392.

[46] Snail S & Papadopoulos S *Cyberlaw@SA: The law of internet in South Africa* (4th ed) Pretoria: Van Schaik (2022) at 307–308.

[47] Snail and Papadopoulos (2022) at 312.

> firstly, the compiling and dissemination of personal information creates a direct threat to an individual's privacy in that privacy includes all those personal facts which a person himself determines should be excluded from the knowledge of others. The right to privacy is infringed if others become acquainted with such information or if it is disclosed to outsider …[48]

Snail and Papadopoulos' observations serve to underline the risk posed by practice directives that require parties to proceedings to upload pleadings that contain confidential information. This confidential information may be hacked by cybercriminals without the party's knowledge and used to commit cybercrimes. It is also observed that the practice directive is silent on the method that the courts should follow to protect confidential or personal information during the use of the CaseLines or e-justice system.

3.2.1 Practice directives relevant to the definition of personal information

It is relevant to consider the background to the implementation of the CaseLines system in civil proceedings. It is contended here that neither of the practice directives that have been issued refer to the protection of personal or confidential information during the process of using CaseLines and online proceedings in the respective courts.[49] Item 3 of Practice Directive 1 of 2020 requires parties to upload pleadings on CaseLines.[50] This practice directive does not provide any assurance that the confidential information uploaded on CaseLines will be protected from unlawful interceptors.[51] The same can be said of Practice Directive 2 of 2020. Subsequent practice directives issued since 2020 also do not show how personal information or confidential information will be safeguarded after the pleadings are uploaded.

Item 7(4) of the Practice Directive 1 of 2021 compels parties to the proceedings to ensure that a relevant "individual document", as well as pleadings, are uploaded to the CaseLines system.[52] This is a gap in the respective directives that should be cured before Rule 18 is implemented. This is contended notwithstanding the fact that the court may be approached to seal the confidential information. Courts should take additional measures to ensure that confidential and personal information is protected before parties resort to court processes in regard to sealing confidential documents. This is so because there are clients who cannot always afford to pay legal practitioners' fees to bring an application to seal the confidential or personal information. Some clients do not have the financial capacity or knowledge to make such an application. The incorporation of an item that shows the methods and steps taken to protect personal or confidential information would put clients and legal practitioners at greater ease. Moreover, the proposed item would show that the courts have made reasonable efforts to protect parties against unlawful interception of private information. This may

[48] Snail and Papadopoulos (2022) at 322.

[49] Practice Directives 1 and 2 of 2020; Practice Directive 2 of 2022.

[50] Item 3 of Practice Directive 1 of 2020.

[51] Practice Directive 1 and 2 of 2020; Practice Directive 1 of 2021; Practice Directive 2 of 2022.

[52] Practice Directive 2 of 2022.

increase trust in courts' commitment to protecting the personal information of litigants and clients.

3.2.2 Section 5 of the POPI Act

It is pertinent to consider section 5 of the POPI Act in the context of the founding affidavits and summonses that contain personal information such as clients' identity numbers. This stipulation deals with the processing of personal information that relates to "data subjects". The interpretation of "data subjects" shows that clients' personal information falls within the ambit of section 5 of the POPI Act. This is so because founding affidavits form part of the pleadings that are uploaded to the CaseLines system in terms of the practice directives. It is argued that the term "processing" denotes that the uploading of the files on the CaseLines falls within the ambit of "a lawful processing", according to this provision.

Section 5(i) states [the applicants have a right] "to institute civil proceedings regarding the alleged interference with the protection of his, her or its personal information as provided for in section 99…". This stipulation is relevant *in casu* because when there is a cybercriminal who hacks a client's personal information, such a client may bring an action for damages resulting from the hacking of his or her personal information.

It is argued the incorporation of the item in the practice directive will protect not only the client but so too the registrar, who is entrusted with a duty to ensure that the data or pleadings are uploaded. The registrar of the court may be sued if no measure is taken to protect the personal information of the client. Roos indicates that, in compliance with the law, there must a "legitimate" reason.[53] The lawful processing is entrenched in the stipulation of section 9 of the Constitution, which enforces the shield of the right to privacy.

3.2.3 Section 11 of POPI Act

Section 11 of the POPI Act permits the processing of information when consent is given by the clients. The question arises: Is consent a complete waiver of the right to claim protection of personal information in civil proceedings? This question is answered in the negative because the mere fact that the client consents to the processing of personal information by uploading the pleading on CaseLines does not necessarily mean that the client may not sue when there is unlawful interception and he or she subsequently suffers damages due to the use of such personal information. Stringent measures should be taken to protect the personal information in pleadings that are uploaded on the CaseLines or e-justice system (when the latter is implemented).

[53] Van der Merwe et al. (2021) at 402.

3.3 Section 42 of RICA

It is important briefly to consider section 42 of RICA. This provision prevents the disclosure of personal information obtained during "the performance of his/her [the person who works with confidential information that is stored electronically] duties" unless the law requires such disclosure. This section is important because the registrars and clerks of the respective court receive personal information filed online by legal practitioners, information which they are precluded from disclosing.

This provision is included because, should there be an unlawful interception of information, the registrars may be held accountable and even sued if the information is used to commit cybercrimes. The case of *Amabhungane Centre for Investigation Journalism NPC v Minister of Justice*[54] affirms that information which is shared between legal practitioners and their clients is entitled to be protected.[55] It is common cause that pleadings such as founding affidavits require clients to disclose aspects of their personal identity, including identity numbers.[56] A reasonable question to consider is whether there is still a need to incorporate personal information such as identity documents in, for example, Rule 3A applications.

This question is answered in the negative because cybercrime has increased since the rules were drafted. This is said because the Cybercrimes Act was passed only in 2020, whilst the Rules were drafted in 2009. There is definitely a very big difference between 2009 and 2020 because much has happened since then. An example is the case of *Fourie v Van Der Spuy,*[57] where unlawful interceptors hacked emails and gave payment instructions to the legal practitioners in regard to money of the client's which was kept in a trust account. The Court ordered the legal practitioners to pay the amount that was paid to the hacker, in this instance more than a million rand. The case is important because it illustrates that hackers can obtain any personal information stored or filed in the CaseLines or e-justice system. It is thus submitted that there is a need to take stringent measures to prevent the interception of private information.

An item should also be incorporated into the practice directive to protect the courts and legal practitioners from being sued by clients. Some authors assert that section 42 of RICA is important in civil proceedings because it prevents the registrars and clerks of the court "from disclosing confidential information that they become aware of while doing their work".[58] It appears that the interception of affidavits with clients' signatures, which are uploaded to CaseLines, could have dire consequences for legal practitioners' clients. For example, the hackers may forge a client's signature and commit fraud or cyberfraud, which taints the good reputation of the client.

---

[54] *Amabhungane Centre for Investigative Journalism NPC v Minister of Justice* 2021 (3) SA 246 (CC).

[55] *Amabhungane (*2021) at para 157.

[56] Rule 3A of the Uniform Rules of Court of 2009.

[57] 2020 (1) SA 560 (GP).

[58] Mabeka NQ "A positive path towards a digital system"in Van der Merwe D et al. *Information and communications technology law* (3rd ed) Durban: LexisNexis (2021) at 702.

This is evinced in *Global & Local Investments Advisors (Pty) Ltd v Fouche,*[59] where hackers sent an email with the clients' initials and gave an instruction for payment, whereas the mandate required the signature of the client.[60] The client was not aware of this instruction, and when he learnt of it, sued the investors for the money paid to the hackers.[61] The Supreme Court of Appeal confirmed that there was a duty on Global & Local Investments to conform to the mandate and that this was evidently not fulfilled because the initials which the hackers used did not constitute a signature.[62] This case demonstrates that cybercriminals are becoming more sophisticated and that there is a need to take stringent measures in practice to protect clients' information.

4 THE IMPACT OF CONFIDENTIALITY AND PERSONAL INFORMATION IN RULE 35 OF THE UNIFORM RULES OF COURT, 2009

The protection of personal information is intertwined with the application of Rule 35, given that this rule compels a party to the proceedings to discover information that is relevant to the trial. If this rule is not complied with, there is a punitive effect on the party who refuses to discover, because the evidence that is not discovered is not admitted in trial proceedings. It is evident that from time to time practitioners may be required to discover confidential or personal information which they are reluctant to disclose. The same principle of discovery applies in the Magistrates' Court Rules in terms of Rule 23.

The courts have linked the application of the rule with the right to confidentiality in various cases. *Waldeck NO and Others v The Land and Agricultural Development*[63] is an example. The Court in this instance had to decide whether documents that ought to have been discovered but which were claimed to be confidential should be disclosed. The Court compelled the respondent to discover the documents that were referred to in the founding affidavit regardless of the claim for confidentiality.[64] It appears that the Court followed a very strict approach in the application of the rule. Similarly, in the case of *Think Holdings Limited v Wesbank a Division of FirstRand Bank Limited*,[65] the Court forced the party to the proceedings to discover, notwithstanding the fact that there was a claim for confidentiality.[66] Once again, this case shows the strict approach that the courts take in applying Rule 35.

---

[59] *Global & Local Investments Advisors (Pty) Ltd v Fouche`* 2021 (1) SA 371 (SCA) (hereafter *Global & Local Investments Advisors* 2021).

[60] *Global & Local Investments Advisors* (2021) at paras 2–4.

[61] *Global & Local Investments Advisors* (2021) at para 3.

[62] *Global & Local Investments Advisors* (2021) at para 14.

[63] *Waldeck NO & Others v The Land and Agricultural Development* (4013/18) [2019] ZAMPMHC 4.

[64] *Waldeck* (2019) at paras 45–49 and 70.

[65] *Think Holdings Limited v Wesbank a Division of FirstRand Bank Limited* (36661/2015) [2021] ZAGPJHC 110.

[66] *Think Holdings Limited* (2021) at para 19.

In *Democratic Alliance and Others v Mkhwebane*,[67] the Supreme Court of Appeal was asked to enforce the application for Rule 35(12) in relation to information contained in the pleadings or affidavits.[68] It was argued that the information in Mkhwebane's founding affidavit deserved to be protected.[69] The Court confirmed that it had the discretion to decide whether or not to waive the strict application of the rule. According to the Court, it was satisfied that the information in question ought to be discovered. Similarly, in *Caxton and CTP Publishers and Printers Limited v Novus Holding Limited*,[70] information regarded as privileged was incorporated in the answering affidavit.[71] The Supreme Court of Appeal averred that discovery is crucial where the documents sought to be protected are important for the proceedings or litigation.[72] Furthermore, when one party refers to a document in the pleadings which is required to be discovered, it prompts the strict application of the rule in the proceedings.[73] The Court further held that "permitting the production of confidential documents subject to appropriate limits, is now firmly established in our law".[74] The decision of the Supreme Court of Appeal further illustrates the strict and narrow application of the rule in civil proceedings.

There is no doubt that the various courts concur when dealing with the application of Rule 35. They compel parties to discover regardless of the claim of confidentiality. It appears that legal scholars also support the courts in the application of Rule 35 in civil procedure. For example, Cassim states that "in the present electronic age, many lawyers are using their computers and digital media to store their files and comments. This leads to discovery by electronic means or electronic discovery, which can be distinguished from traditional paper discovery …"[75] Other scholars, such as Theophilopoulos et al., indicate that:

> [t]he discovery affidavit must be deposed to by the actual party or, if the party is a body corporate, firm or association, the affidavit must be made by a member or employee who has personal knowledge of the matter and the issues. Only in exceptional circumstances will an attorney be allowed to depose a discovery affidavit on behalf of a client …[76]

These scholars suggest that the test is whether evidence must be led to prove that the documents that are discovered are authentic.[77] This assertion is in line with the application of the rules of evidence in civil procedure. The scholars also affirm that the

---

[67] *Democratic Alliance and Others v Mkhwebane* (2021) 3 SA 403 (SCA).

[68] *Democratic Alliance* (2021) at paras 1, 11, 15, 16, 20–38, 44, and 46–47.

[69] *Democratic Alliance* (2021) at paras 1 and 2.

[70] *Caxton and CTP Publishers and Printers Limited v Novus Holding Limited* 2022 (2) All SA 299 (SCA).

[71] *Caxton and CTP Publishers* (2022) at paras 8 and 9.

[72] *Caxton and CTP Publishers* (2022) at para 70.

[73] *Caxton and CTP Publishers* (2022) at para 15.

[74] *Caxton and CTP Publishers* (2022) at para 81.

[75] Cassim F "The use of electronic and cloud-computing technology by lawyers in practice: Lessons from abroad" 2017 42(1) *Journal for Juridical Science* at 21.

[76] Theophilopoulos C et al. *Fundamental principles of civil procedure* (2020) at 351.

[77] Theophilopoulos et al. (2020) at 351.

same principle applies to Rule 23 of the Magistrates' Courts Rules.[78] Van Loggerenberg,[79] Harms, [80] Van Dorsten,[81] and Hoornstra and Liethen[82] support this view and affirm that discovery is a crucial aspect of litigation.

Rule 23 of the Magistrates' Courts Rules is similar to Rule 35 and therefore does not warrant detailed discussion. The only difference between the two rules is that the former is applied in the lower courts whereas the latter is applied in superior courts such as high courts. Van Blerk argues that discovery is an important process in litigation, asserting that "our courts have held that where a document has been prepared with the definite purpose of submission to legal advisors, albeit that is it is not the only purpose, it is privileged from disclosure".[83] He justifies his argument with reference to the case law.[84] It appears that the decision in the case to which Van Bleck refers is an exception to the above-mentioned cases.

Broodryk argues that it is important to discover the documents that are necessary for the litigation.[85] He highlights the consequences of non-compliance with Rule 35, and indicates that courts disadvantage those who refuse to discover for whatever reason by eliminating documents that should have been discovered.[86] Such documents are not admitted as evidence in civil proceedings if there is non-compliance with Rule 23 of the Magistrates' Courts Rules. Alternatively, the court may strike out or dismiss the matter if there is non-compliance with the rule.[87] Pete et al. indicate that discovery reduces the number of disputes that may arise where there is non-compliance with the rules of discovery.[88] Furthermore, there are no surprises in store for parties to the proceedings in the event of non-compliance.[89] Swales argues that practitioners seldom use electronic means of discovery, even though this option is available to them.[90] He argues the rules

[78] Theophilopoulos et al. (2020) at 351.

[79] Van Loggerenberg DE *Jones & Buckle: The practice of the magistrates in South Africa* (10th ed) Cape Town: Juta (2017) at 16.

[80] Harms D *Civil procedure in the magistrates courts* Durban: LexisNexis (2016) at C10–100.

[81] Van Dorsten J "Discovery of electronic documents and attorneys obligations" (2012) 1 *De Rebus* at 34.

[82] Hoornstra CD and Liethen MA "Academic freedom and civil discovery" (1983) *Heinonline* 113 at 115–117.

[83] Van Blerk P *Preparation for civil trials* Cape Town: Juta (2019) at 77–82.

[84] Van Blerk (2019) at 82.

[85] Broodryk T *Eckard's principles of civil procedure in the Magistrates' Court* (6th ed) Cape Town: Juta (2019) at 189.

[86] Broodryk (2019) at 189.

[87] Broodryk (2019) at 189.

[88] Pete S, Hulme D, du Plessis M, Palmer R & Sibanda O *Civil procedure: A practical guide* (3rd ed) Oxford: Oxford University Press (2017) at 265.

[89] Pete et al. (2017) at 265.

[90] Swales L "The Protection of Personal Information Act and data de-identification" (2021) 1 *South African Journal of Science* at 2–3.

should be amended to accommodate electronic disclosure in compliance with the rule. Other authors concur with Swales's averment that it is time to use electronic discovery in civil procedure.[91] It is observed that South African authors and courts view the process of discovery as a crucial one in civil procedure.

Though the importance of discovery is irrefutable, it must be noted that there is a major risk in the light of evolving technology because there are unlawful interceptors who wait for opportunities to commit cybercrimes. As a result, the personal information contained in pleadings may be hacked and used to commit cyberfraud or other cybercrimes, which can have dire consequences for legal practitioners' clients. Evidently, there is a need to take strict measures to protect personal information in pleadings that are uploaded online. This calls for an amendment in the manner of providing personal information to the courts in compliance with Rule 35 of the Uniform Rules of Court and Rule 23 of the Magistrates' Court Rules, without including personal information such as identity numbers of the applicant[s] or legal practitioners' clients in the discovered documents. The question then arises of how this amendment would be made. The answer thereto is provided in the recommendations made in this article.

5 A BRIEF COMPARISON OF SOUTH AFRICA AND THE UNITED KINGDOM

As far as confidentiality in civil procedure in the United Kingdom (UK) is concerned, the relevant practice directions are 31A, 31B and 57. Practice Direction 31 provides for the general process governing the disclosure of information in civil proceedings.[92] Practice Direction 31A deals specifically with electronic disclosure.[93] The relevant provision of Practice Direction 31A is Item 2A. Item 2A.1 states as follows:

> Rule 31.4 contains a broad definition of a document. This extends to *electronic documents, including e-mail and other electronic communications, word processed documents and databases*. In addition to documents that are readily accessible from computer systems and other electronic devices and media, the definition covers those documents that are stored on servers and back-up systems and electronic documents that have been "deleted". It also extends to additional information stored and associated with electronic documents known as metadata …[94]

This provision demonstrates that data which is stored and disclosed in the UK falls within the ambit of this direction. The data may include confidential or personal information that ought to be shielded. This practice direction is relevant to electronic documents that are filed and disclosed during litigation because solicitors store confidential information that may be necessary for litigation and which the other party to the civil proceedings may ask to have disclosed.

Unlike Item 18 of South Africa's E-Rules, the UK's Practice Direction 31 does not expressly contain an item or provision that shows how clients' personal information

[91] Mabeka NQ "A positive path towards a digital system" in Van der Merwe D et al. *Information and communications technology law* (3rd ed) Durban: LexisNexis (2021) at 687.

[92] Item 2A of Practice Direction 31.

[93] Practice Direction 31A.

[94] Item 2A.1 of Practice Direction 31. Emphasis added.

that is electronically filed will be protected. For example, there is no specific provision or item in the UK Practice Direction 31 that illustrates to legal practitioners and their clients the type of software that is used to protect personal information that is electronically filed from hackers. It appears that the UK may need to consider incorporating a clause in the practice direction that specifies the level of protection required for electronic data which is filed, disclosed, or stored by the civil courts during litigation. When this practice direction is compared with Item 18, it is observed that both seek to regulate electronic communications in civil procedure matters. Item 31.4(5) sets out certain conditions that must be met when claiming confidentiality. Item 31.4 provides as follows:

> If the disclosing party wishes *to claim that he has a right or duty to withhold a document,* or part of a document, in his list of documents from inspection (see rule 31.19(3)), he must state in writing:
>
> (1) that he has such a right or duty, and
>
> (2) the grounds on which he claims that right or duty …[95]

The provision above illustrates that parties to the proceedings may claim confidentiality just as is the case with Item 18 of the E-Rules in South Africa. Practice Direction 31B is also crucial in protecting electronic communication which is stored or distributed during civil litigation in the United Kingdom. This is so because it defines electronic documents and the disclosure of data that may be viewed as personal information or confidential. Item 31B(5)(2) states:

> (2) "Disclosure Data" *means data relating to disclosed documents, including for example the type of document, the date of the document, the names of the author or sender and the recipient, and the party disclosing the document*;
>
> (3) "Electronic Document" means *any* document held in *electronic form.* It includes, for example, *email and other electronic communications such as text messages and voicemail, word-processed documents and databases, and documents stored on portable devices such as memory sticks and mobile phones*. In addition to documents that are readily accessible from computer systems and other electronic devices and media, it includes documents that are stored on servers and back-up systems and documents that have been deleted. It also includes metadata and other embedded data, which is not typically visible on screen or a printout …[96]

The above denotes that it is the intention of the UK's courts to regulate electronic communication which is disclosed or stored during litigation. The narrow interpretation of "electronic document" in Item 3 shows that confidential or personal information ought to be preserved and protected. Surprisingly, although there is a clear intention to regulate electronic communication in the United Kingdom, there is no specific provision in the above practice direction that is similar to Item 18 of the E-Rules, which protects confidential or personal information by making provision

[95] Emphasis added.

[96] Practice Direction 31B(5)(2). Emphases added.

for an application that the court seal the said information. It is perhaps time for the UK to consider incorporating an express provision that puts solicitors at ease in as far as the protection of personal or confidential information is concerned, just as is the case with the provisions of Item 18 of the E-Rules.

Unlike in the UK, Item 1 of the South African E-Rules has two separate definitions of a document in the context of the stipulations of the Electronic Communications and Transactions Act 25 of 2002, which spell out pleadings and notices that are filed and served in terms of the respective rules of various courts. It is observed that the practice direction does not narrow down the meaning of "data" to expressly include pleadings and notices. It appears that this is a gap which the UK should close in practice.

It is important to consider Practice Direction 57, which deals with disclosure in regard to business and property. This is applicable in civil procedure because a business, as a juristic person with legal standing, may institute civil proceedings for damages suffered and be involved in litigation. Consequently, this practice direction is considered here because there is a need, too, to protect data in civil proceedings where confidential documents are significant for litigation on business matters. Practice Direction 57 regulates and preserves confidentiality in civil proceedings. Item 15 of Practice Direction 57 is significant in this regard. It states:

> If there are material concerns over the confidentiality of a document (whether the confidentiality benefits a party to the proceedings or a third party), *the court may order disclosure to a limited class of persons, upon such terms and subject to such conditions as it thinks fit*. The court may make further orders upon the request of a party, or on its own initiative, varying the class of persons, or varying the terms and conditions previously ordered, or removing any limitation on disclosure …[97]

This provision is similar to Item 18 of the E-Rules because they both seek to preserve confidentiality during the proceedings. More importantly, both require the courts to use their discretion to protect confidential documents. This is, however, not enough. It is observed that Item 15 of the practice direction does not necessarily refer to electronic communications. Item 18 of the E-Rules concerns the protection of confidential documents that are filed electronically. Furthermore, the court, according to the above practice direction, may use its discretion to limit the extent of disclosure during litigation. Ambrose et al. argue that legal practitioners ought to always protect the interests of their clients at all times. In addition, UK courts may restrict the disclosure of confidential information. It is important to highlight the relevant provision of the practice direction that governs disclosure in the UK.

The UK courts have endorsed the enforcement of the disclosure of documents during litigation. The Court in *Hilton v Baker Booth and Eastwood*[98] had to determine

[97] Item 15 of Practice Direction 57. Emphasis added.

[98] *Hilton v Baker Booth and Eastwood* 2005 UKHL 8.

whether information relating to clients' bankruptcy and criminal conviction fell within the ambit of confidential information. In coming to its conclusion, it stated:

> The relationship between a solicitor and his client is one in which the client reposes trust and confidence in the solicitor. It is a fiduciary relationship. But not every breach of duty by a fiduciary is a breach of fiduciary duty ...[99]

The Court in this case held that information relating to a history of criminal activities such as fraudulent trading and getting involved in management whilst there is a pending bankruptcy case; did not deserve protection because such shield would have frustrated the court in properly applying its mind in making a final decision.[100]

The Court went further and decided that the terms and conditions of the contractual obligations between the client and the solicitor determine the level of preserving confidentiality.[101]

In the case of *Digicel (St Lucia) Ltd & Ors v Cable & Wireless Plc & Ors*,[102] the Court emphasised that disclosure of documents is necessary for litigation. In applying Practice Direction 31, it set out three important aspects of disclosure.[103] First, the party requesting the other party to disclose must ensure that the information is relevant. Secondly, the Court held that such information must hinder the case in an adverse manner. Thirdly, a question should be asked whether such information should really be disclosed. In *Earles v Barclays Bank Plc,*[104] the Court held that solicitors are compelled to disclose electronic documents that are pertinent to litigation. If they fail to do so, the failure amounts to "gross incompetence".[105]

The UK courts show the significance of protecting personal information in civil procedure when applying the disclosure rule. The discretion of the courts in granting orders for disclosure was highlighted in *Lisle-Mainwaring v Associated Newspapers Ltd*.[106] The Court had to apply Practice Direction 31, and stated that:

> [i]f a court concluded that the respondent to the application had failed to comply with the order for standard disclosure, then it will "usually" make the appropriate order: see paragraph 5.4 of PD 31A. If, on the other hand, the court is not so persuaded, then it may be more difficult for the applicant to obtain an order for specific disclosure. But it is not impossible. That is because, as paragraph 5.5(1) makes clear, in an appropriate case, the court may make an order for disclosure which is wider than the constraints governing

---

[99] *Hilton* (2005) at para 29.

[100] *Hilton* (2005) at paras 8, 14 22 and 29.

[101] *Hilton* (2005) at para 30.

[102] *Digicel (St Lucia) Ltd &Ors v Cable & Wireless Plc & Ors* 2008 England and Wales High Court (Chancery Division).

[103] *Digicel* (2008).

[104] *Earles v Barclays Bank Plc* 2009 EWHC 2500 (QB).

[105] *Earles* (2009) at para 71.

[106] *Lisle-Mainwaring v Associated Newspapers Ltd* 2018 EWCA Civ 1470.

> standard disclosure and could even extend to an old-fashioned "train of enquiry" exercise (the unlamented *Peruvian Guano* test) …[107]

The Court was of the view that parties could not be compelled to disclose the electronic documents that were required to be discovered. This case shows the flexible approach of the UK courts in disclosure matters.

In *Phone 4 U Ltd (in administration) v EE Ltd and Others*,[108] the Court dealt specifically with the application of Practice Direction 31. The issue arose of whether or not emails that are archived on personal devices could be disclosed. The Court averred that the practice direction is interpreted in a manner that permits courts to use their discretion in relation to the extent to which parties should disclose personal or confidential information. This appears to be similar to the approach followed by South African courts because they also use their discretion, but in some instances tend to apply a strict approach when considering Rule 35 matters and reject evidence which is not disclosed, as in *Lewis Group Ltd v Woolman and Others*.[109] In another recent case, *Gorbachev v Guriev,*[110] the Court put emphasis on the discretion that courts have in compelling parties to disclose electronic documents.[111]

Scholars in the UK such as Andrew assert that there is an additional restriction in the disclosure during the application of Practice Direction 31.[112] Andrew states:

> [A] party to whom a document has disclosed may use the document only for the purpose of the proceedings in which it is disclosed, except where the document has been read to or by the court or referred to at a hearing which has been held in public …[113]

Other such as Ambrose et al. concur with the decision in the *Hilton case* that:

> A solicitor has a duty of single-minded loyalty to his clients, and a duty to respect his clients' confidences do have their roots in the fiduciary nature of the solicitor-client relationship. But they may have to be moulded and informed by the terms of the contractual relationship …[114]

These authors agree with South African courts that solicitors ought to disclose information that is important for litigation and which may hinder the plaintiff's case or corroborate the evidence of the defendant.[115] Ambrose et al. support the notion that Practice Direction 31 includes electronic documents as defined in the practice

---

[107] *Lisle* (2018) at para 36.

[108] *Phone 4U Ltd (in administration) v EE Ltd and Others* 2022 (1) All (ER).

[109] *Lewis Group Ltd v Woolman and Others* (2) 2017 1 All SA 231 (WCC) at para 4.

[110] *Gorbachhev v Guriev* 2023 (2) All (ER) 809.

[111] *Gorbachlev* (2023) at para 93.

[112] Andrew N *Court proceedings, arbitration & mediation* (2nd ed) Cambridge: Intersentia (2019) at 267.

[113] Andrew (2019) at 267.

Ambrose H et al. *Blackstone's civil practice* (21st ed) Oxford: Oxford University Press (2021) at 491; Hilton (2005) at para 30.

[115] Ambrose et al. (2021) at 962.

direction.[116] Ambrose et al. further argue that the plaintiff may ask the court to limit the extent of the information to be disclosed due to confidentiality. This is akin to Item 18 of the E-Rules because a court may be asked to seal confidential information.

Consequently, the UK has similarities with South Africa in applying the rules of discovery. The courts in both the UK and South Africa use their discretion when asked to grant orders on disclosure. Scholars in both jurisdictions also support the position of the courts. The exception is that Andrew suggests that there is an additional restriction on disclosure, which is highlighted in the above discussion. The restriction that Andrew refers to does not exist in the South African rules and is not used by the civil courts. Suffice it to say that this is the difference between South Africa and the UK.

6 RECOMMENDATIONS

It is contended here that the courts should introduce an encryption method or process to protect personal information that is electronically filed and uploaded online in accordance with the CaseLines system and the E-Rules that will replace the Magistrates' Courts Rules and the Uniform Rules of Court in the respective High Courts. The encryption of these court papers will assure the legal practitioners that their clients' personal information such identity numbers is protected. The registrars should create passwords that should be made available only to legal practitioners who are representing the applicants and respondents and to the judge who is allocated to preside on the matter.

This password should be changed from time to time to limit the risk of unlawful interception. It is submitted that it would mitigate the risk of unlawful intercept if during the trial stage there is a need to refer to personal information, the judge should refer to these only to identify the parties and without necessarily citing the full identity number of the clients. For example, in application proceedings, the judge may simply confirm that the applicant has complied with the rules and provided all the necessary personal information to justify the admission.

7 CONCLUSION

There is no doubt that the courts in South Africa are undergoing transformation by using e-technology to effect court processes. In the process, there is a risk that confidential or personal information may be intercepted by hackers and used for unlawful activities.

This may happen in instances where affidavits or pleadings that contain personal information, such as identity numbers or the physical addresses of legal practitioners' clients, are hacked. It is submitted that the legislature has attempted to protect the clients' personal information or confidential information. This is shown in the provisions of the POPI Act, section 14 of the Constitution, and RICA. The respective rules

[116] Ambrose et al. (2021) at 966.

of courts such as the E-Rules and the Draft Amended Magistrates' Courts Rules attempt to protect personal information which is filed online during litigation.

This article contends, however, that there is not enough protection of confidential or personal information which is uploaded on the CaseLines or E-Justice system. This article calls for the amendment of the Rule 23 of the Magistrates' Court Rules, Rule 35 of the Uniform Rules of Court, Item 18 of the E-Rules, as well as Item 18 of the Draft Amended Magistrates' Courts Rules. These rules should incorporate a clause that confirms that the online system has software that guarantees the protection of personal or confidential information. This would protect and preclude legal practitioners, as well as the courts, from claims for damages suffered by the clients when there is evidence which confirms that there was unlawful interception of the CaseLines or E-Justice system. Lastly, the courts should consider implementing the recommendations that are made in this article.

BIBLIOGRAPHY

Books

Ambrose H et al. *Blackstone's civil practice* (21st ed) Oxford: Oxford University Press (2021)

Andrew N *Court proceedings, arbitration & mediation* (2nd ed) Cambridge: Intersentia (2019)

Broodryk T *Eckard's principles of civil procedure in the Magistrates' Court* (6th ed) Cape Town: Juta &Co Ltd (2019)

Currie I & de Waal J *The bill of rights handbook* (6th ed) Cape Town: Juta & Co Ltd (2014)

Harms D *Civil procedure in the magistrates courts* Durban: LexisNexis (2016)

Pete S, Hulme D, du Plessis M, Palmer R & Sibanda O *Civil procedure: A practical guide* (3rd ed) London: Oxford (2017)

Snail S & Papadopoulos S *Cyberlaw@SA: The law of internet in South Africa* (4th ed) Pretoria: Van Schaik (2022) at 307–308

Theophilopoulos C, van Heerden CM, Boraine A & Rowan A *Fundamental principles of civil procedure* (4th ed) Durban: LexisNexis (2020)

Van Blerk P *Preparation for civil trials* Cape Town: Juta & Co Ltd (2019)

Van der Merwe D et al. *Information and communications technology law* (3rd ed) Durban: LexisNexis (2021)

Van Loggerenberg DE *Jones & Buckle: The practice of the magistrates in South Africa* Cape Town: Juta &Co Ltd (2017)

Chapters in books

Mabeka NQ "A positive path towards a digital system" in Van der Merwe D, Roos A, Eiselen GTS, Nel SS, Erlank W & Mabeka NQ (3rd ed) *Information and communications technology law* Durban: LexisNexis (2021)

Roos A "Data privacy law" in Van der Merwe D, Roos A, Eiselen GTS, Nel SS, Erlank W & Mabeka NQ *Information and communications technology law* (3rd ed) Durban: LexisNexis (2021)

Van Der Merwe D "Criminal law" in Van der Merwe D, Roos A, Eiselen GTS, Nel SS, Erlank W & Mabeka NQ *Information and communications technology law* (3rd ed) Durban: LexisNexis (2021)

Journals

Cassim F "Addressing the growing spectre of cybercrime in Africa: evaluating measures adopted by South Africa and other regional role players" (2011) *The Comparative and International Law Journal of Southern Africa* 123–138

Cassim F "The use of electronic and cloud-computing technology by lawyers in practice: Lessons from abroad" (2017) Vol 42(1) *Journal for Juridical Science* 19–40

Cassim F and Mabeka N "The Africanisation of South African civil procedure: The way Forward" (2019) *Journal of Law, Society and Development* 1–20

Hoornstra CD and Liethen MA "Academic freedom and civil discovery" (1983) *Heinonline* 113–117

Mabeka NQ "An analysis of the implementation of the CaseLines System in South African courts in the light of the provisions of section 27 of the Electronic Communications and Transactions Act 25 of 2002: A beautiful dream to come true" (2021) *Potchefstroom Electronic Law Journal* 1–31

Snail S "Cybercrimes in South Africa – Hacking, cracking, and other unlawful online activities" (2009) 1 *Journal of Information, Law & Technology* at 4–5

Swales L "The Protection of Personal Information Act and data de-identification" (2021) *South African Journal of Science* 1–3

Van Dorsten J "Discovery of electronic documents and attorneys obligations" (2012) *De Rebus* 1–36.

Cases

All G2 G Ltd and Others v van Rensburg and Others (59644/2020) [2021] ZAGPPHC 425

Amabhungane Centre for Investigative Journalism NPC v Minister of Justice 2021 (3) SA 246 (CC)

Arena Holdings Pty Ltd t/a Financial Mail and Others v South African Revenue and Others 2023 (5) SA 319 (CC)

Bernstein v Bester 1996 (2) SA 751 (CC)

Caxton and CTP Publishers and Printers Limited v Novus Holding Limited 2022 (2) All SA 299 (SCA)

Democratic Alliance and Others v Mkhwebane 2021 (3) SA 403 (SCA)

Digicel *(St Lucia) Ltd & Ors v Cable & Wireless Plc &Ors* 2008 England and Wales High Court (Chancery Division)

Earles v Barclays Bank Plc 2009 EWHC 2500 (QB)

Fourie v Van Der Spy 2020 (1) SA 560 (GP)

Genesis One Lighting v Jamieson and Others (19/3212) [2019] ZAGP JHC 93

Global & Local Investments Advisors (Pty) Ltd v Fouche` 2021 (1) SA 371 (SCA)

Gorbachev v Guriev 2023 (2) All (ER) 809

Helen Suzman Foundation v Judicial Service Commission 2018 (4) SA 1 (CC)

Hilton v Baker Booth and Eastwood 2005 UKHL 8

Lewis Group Ltd v Woolman and Others 2017 (1) All SA 231 (WCC)

Lisle-Mainwaring v Associated Newspapers Ltd 2018 EWCA Civ 1470

NM V Smith 2007 (5) SA 250 (CC)

Phone 4U Ltd (in administration) v EE Ltd and Others 2022 (1) All (ER)

Replication Technology Group and Others v Gallo Africa Limited and Others 2009 (5) SA 531 (GSJ)

South African Airways Soc v BDFM Publishers Pty Ltd and Others 2016 (1) All 860 (GJ)

Think Holdings Limited v Wesbank a Division of FirstRand Bank Limited (36661/2015) [2021] ZAGPJHC 110

Tshabalala-Msimang v Makhanya & Others 2008 (6) SA 102 (W)

Waldeck NO and Others v The Land and Agricultural Development (4013/18 2019) ZAMPMHC 4

Constitution

Constitution of the Republic of South Africa of 1996

Legislation

Electronic Communications and Transactions Act 25 of 2002

Legal Practice Act 28 of 2014

Protection of Personal Information Act 4 of 2013

Regulation of Interception of Communications and Provisions of Communication-Related Information Act 70 of 2002

Rules

Draft Amended Magistrates' Courts Rules, 2021

E-Rules: Draft Amended Uniform Rules, 2021

Uniform Rules of Court, 2009, as amended

Magistrates' Court Rules, 2010, as amended

Practice Direction and Practice Directives

Practice Directive 1 of 2020

Practice Directive 2 of 2020

Practice Directive 2 of 2022

Practice Directive 1 of 2023

Directive 2 of 2022

Practice Direction 31

Practice Direction 57

Internet sources

Lenaert-Bergmans, B "Understanding the differences between spoofing vs phishing" (2023) available at https://www.crowdstrike.com/cybersecurity-101/attack-types/spoofing-vs-phishing/ (accessed 9 January 2024)

Strom S & Earhart R "Is there a difference between confidentiality and privacy?" (2024) available at https:// www.findlaw.com/criminal/rights/is-there-a-difference-between-confidentiality-and-privacy.html (accessed 8 January 2024)

The Judiciary of South Africa available at https://www.courtonline.judiciary.org.za (accessed 11 January 2024)