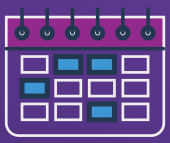
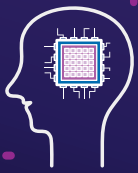


COMPENDIUM OF CASE LAW RELATING TO DIGITAL FREEDOMS

Freedom of Expression, Access to Information, Privacy, Data Protection, Right to Erasure and Anti-SLAPP Principles



Prepared as a practical litigation and advocacy resource for Human Rights Lawyers, Public Interest Litigators, Civil Society Organisations, Journalists, Online Content Creators and Human Rights Defenders.

ACKNOWLEDGEMENTS

This compendium was developed as part of the author's Bertha Challenge work titled "Pushing Back Against State Collusion with Telecommunications Companies to Undermine Freedom of Expression and the Right to Privacy in Zimbabwe." The framing recognises that digital freedoms are not only doctrinal rights; they are lived protections for journalists, civil society actors, online content creators, human rights defenders and ordinary citizens who rely on digital spaces to speak, organise, investigate and hold power to account.

The work is informed by the broader concern that restrictions on freedom of expression, privacy and access to information may be enabled through a combination of laws, administrative controls, surveillance practices and the involvement or cooperation of private actors, including telecommunications companies and digital service providers. The compendium therefore brings together Zimbabwean, regional and comparative authorities that can support litigation, advocacy and public education in defence of digital freedoms.

Special thanks are extended to the Zimbabwe Human Rights NGO Forum, which served as the host organisation for the Bertha Challenge fellowship. The Forum provided an important institutional platform for the development, publication and dissemination of this compendium, and created opportunities for the author to work with its members and partners in advancing digital rights, freedom of expression, privacy and accountability in Zimbabwe.

The author also acknowledges the support of the Bertha Foundation and the broader Bertha Challenge community, whose commitment to movement lawyering, investigative advocacy and accountability made this work possible.

BERTHA FOUNDATION

Zimbabwe HUMAN RIGHTS NGO Forum 25

CONTENTS

04 **Chapter 1:** Background and Legal Framework

09 **Chapter 2:** Constitutional Applications, Direct Access and Locus Standi

18 **Chapter 3:** Freedom of Expression and Digital Freedoms

27 **Chapter 4:** Access to Information

31 **Chapter 5:** Data Protection and Privacy

38 **Chapter 6:** Right to Erasure / Right to Be Forgotten

49 **Chapter 7:** Strategic Litigation Against Public Participation (SLAPPs)

54 **Bibliography**

CHAPTER 01

Background and Legal Framework

1.1 Purpose and Legal Foundation

This compendium is grounded in the recognition that digital freedoms are no longer peripheral to human rights protection; they are central to the enjoyment of constitutional democracy, civic participation, accountability, and access to justice. Freedom of expression, media freedom, access to information, privacy, data protection, anonymity, encryption, and protection against Strategic Litigation Against Public Participation (SLAPPs) increasingly operate in an interconnected digital ecosystem. The internet has become a primary space through which citizens receive and impart information, journalists investigate public interest issues, civil society organisations mobilise communities, whistleblowers expose wrongdoing, and human rights defenders hold public and private power to account.

At the international level, the normative foundation for these rights is anchored in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights (ICCPR).[1] Article 19 of the ICCPR protects the right to hold opinions without interference and the freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers and through any media. This principle is particularly important in the digital age because expression now occurs not only through newspapers, radio and public gatherings, but also through social media, online journalism, blogs, encrypted messaging platforms, digital archives and citizen reporting.

The same international framework protects privacy. Article 17 of the ICCPR[2] prohibits arbitrary or unlawful interference with privacy, family, home or correspondence. The UN Human Rights Committee has explained that even interference authorised by law may still be arbitrary if it is unreasonable, unnecessary or disproportionate. In the digital context, this protection extends to personal data, communications metadata, digital correspondence, device identifiers, biometric information, online activity, geolocation data and confidential communications. Privacy is therefore not merely an individual interest; it is an enabling right. Without privacy, journalists cannot protect sources, activists cannot organise securely, whistleblowers cannot safely disclose wrongdoing, and ordinary citizens may self-censor for fear of surveillance or retaliation.

The United Nations has also affirmed that the same rights people enjoy offline must be protected online[3], particularly freedom of expression. This principle has become a cornerstone of global digital rights advocacy. It means that States cannot treat the internet as a rights-free zone. Measures such as internet shutdowns, arbitrary blocking of websites, overbroad cybercrime offences, unlawful surveillance, forced disclosure of anonymous users, or disproportionate restrictions on online speech must be tested against the same standards of legality, legitimacy,

1. UN Human Rights Committee, General Comment No. 34 on Article 19: Freedoms of Opinion and Expression, CCPR/C/GC/34, 12 September 2011.
2. UN Human Rights Committee, General Comment No. 16 on Article 17: Right to Privacy, 8 April 1988.
3. UN Human Rights Council, Resolution A/HRC/RES/32/13, The Promotion, Protection and Enjoyment of Human Rights on the Internet, 18 July 2016.

necessity and proportionality that apply to restrictions on offline expression. The UN Office of the High Commissioner for Human Rights[4] has further recognised that privacy is central to the enjoyment of human rights online and offline and is foundational to democratic society.

1.2 Regional African Standards

At the regional level, the African human rights system provides an equally important framework. Article 9 of the African Charter on Human and Peoples' Rights guarantees the right to receive information and the right to express and disseminate opinions within the law. The African Commission's Declaration of Principles on Freedom of Expression and Access to Information in Africa develops this protection further by affirming the rights to freedom of expression, access to information, media freedom, privacy, protection of journalistic sources, and access to the internet. These principles are particularly relevant to African contexts where internet shutdowns, criminal defamation laws, surveillance powers, restrictive accreditation regimes and cybercrime laws have often been used to constrain civic space.

The African Union Convention on Cyber Security and Personal Data Protection[5], commonly known as the Malabo Convention, also provides an important regional framework for data protection, cybersecurity and electronic governance. It reflects the growing recognition that the digital economy and digital governance must be built on trust, lawful processing of personal data, security safeguards, accountability, and respect for fundamental rights. Although implementation across the continent remains uneven, the Convention provides persuasive guidance for courts, regulators and litigators seeking to align domestic cyber and data protection laws with human rights standards.

1.3 Constitutional Framework in Zimbabwe

Within Zimbabwe, the constitutional framework is particularly significant. The Constitution of Zimbabwe Amendment (No. 20) Act, 2013[6] protects privacy under section 57, freedom of expression and freedom of the media under section 61, and access to information under section 62. Section 57 expressly protects individuals against unlawful collection, storage, use or disclosure of personal information. Section 61 protects the freedom to seek, receive and communicate ideas and other information, while section 62 guarantees access to information held by the State where required in the interests of public accountability, and access to information held by any person where required for the exercise or protection of a right. These rights must also be read together with section 44, which places a duty on the State and every person to respect, protect, promote and fulfil constitutional rights, and section 85, which broadens standing for constitutional litigation, including public interest litigation.

The Zimbabwean Constitution also provides an important limitation framework. Under section 86[7], fundamental rights may be limited only by a law of general application and only to the extent that the limitation is fair, reasonable, necessary and justifiable in a democratic society based on openness, justice, human dignity, equality and freedom. This means that restrictions on digital rights must not be vague, arbitrary, excessive or disproportionate. Laws criminalising online

4. OHCHR, International Standards on Privacy in the Digital Age.
5. African Union Convention on Cyber Security and Personal Data Protection, adopted 27 June 2014.
6. Constitution of Zimbabwe Amendment (No. 20) Act, 2013, ss 44, 57, 61, 62 and 85.
7. Constitution of Zimbabwe Amendment (No. 20) Act, 2013, s 86.

speech, authorising surveillance, limiting access to information, regulating media accreditation, or enabling data processing must therefore meet constitutional standards of legality, necessity and proportionality.

The Cyber and Data Protection Act [Chapter 12:07][8] gives legislative expression to aspects of the right to privacy and data protection in Zimbabwe. Its object includes increasing cybersecurity in order to build confidence and trust in the secure use of information and communication technologies. The Act regulates the processing of personal information and recognises important data subject rights,[9] including the right to be informed of the use of personal information, the right to access personal information held by a data controller or processor, the right to object to processing, the right to correction of false or misleading information, and the right to deletion of false or misleading data. These protections are central to emerging litigation on data privacy, data breaches, biometric systems, surveillance, platform accountability and the right to erasure.

1.4 Right to Erasure and Digital Permanence

The right to erasure, or the right to be forgotten, is an emerging aspect of privacy and data protection. It recognises that individuals should not always remain indefinitely exposed to outdated, irrelevant, excessive or misleading personal information, particularly where continued online accessibility causes disproportionate harm. However, the right is not absolute. It must be balanced against freedom of expression, media freedom, open justice, historical records, public accountability and the public's right to know.

Comparative jurisprudence, including cases such as Google Spain,[10] **Biancardi v Italy**[11] and **Hurbain v Belgium**[12], illustrates that courts are more willing to order de-indexing or limited erasure where search engines amplify access to personal data, but they are more cautious where the remedy would alter journalistic archives, court records or information of continuing public interest. The compendium captures this delicate balance between privacy, digital permanence and public interest information.

1.5 Access to Information and Democratic Accountability

Access to information is another core pillar of this compendium. It enables citizens, journalists, CSOs and affected communities to scrutinise government conduct, expose corruption, monitor elections, demand service delivery, and participate meaningfully in democratic processes. The Freedom of Information Act [Chapter 10:33][13] was enacted to give effect to the constitutional right of access to information and to repeal the Access to Information and Protection of Privacy Act. However, access to information litigation continues to raise difficult questions about secrecy, national security, institutional confidentiality, privacy, electoral integrity and the exhaustion of statutory remedies.

For public interest lawyers, the central principle is that secrecy must be justified; it cannot be presumed. Where public authorities refuse disclosure, they must show that the refusal is lawful, necessary and proportionate. This is particularly important where access to information is

8. Cyber and Data Protection Act [Chapter 12:07], long title and objects provisions.
9. Cyber and Data Protection Act [Chapter 12:07], provisions on data subject rights, including access, objection, correction and deletion.
10. This compendium, Chapter 5: Right to Erasure/Be Forgotten Cases, including discussion of Google Spain, Biancardi v Italy and Hurbain v Belgium.
11. Biancardi v Italy App no 77419/16 (ECtHR, 25 November 2021), on de-indexing, journalistic archives and proportionality.
12. Hurbain v Belgium App no 57292/16 (ECtHR, Grand Chamber, 4 July 2023), on anonymisation of online news archives and balancing privacy with press freedom.
13. Freedom of Information Act [Chapter 10:33].

necessary to expose corruption, monitor public procurement, scrutinise elections, assess public service delivery, or protect other constitutional rights.

1.6 Strategic Litigation Against Public Participation (SLAPPs)

Freedom of expression and access to information are also closely connected to protection against SLAPPs. SLAPPs are abusive lawsuits[14] or threats of legal action designed to silence public participation, investigative reporting, whistle-blowing, activism and criticism on matters of public interest. They are often framed as defamation claims, privacy claims, data protection complaints, confidentiality actions, harassment claims, intellectual property disputes or commercial claims. Their true purpose is frequently not to vindicate legitimate rights, but to intimidate critics, drain resources, delay publication, remove information from the public domain, and create a chilling effect. The OHCHR has described SLAPPs as lawsuits or threats that use abusive litigation tactics with the aim or effect of suppressing public participation and critical reporting on matters of public interest.

International concern about SLAPPs has grown significantly. The Council of Europe adopted Recommendation CM/Rec(2024)2[15] on countering SLAPPs in April 2024, warning of their chilling effect on freedom of expression and public participation. The European Union has also adopted an Anti-SLAPP Directive[16] to protect persons who engage in public participation from manifestly unfounded or abusive court proceedings. Although these instruments are not binding in Zimbabwe, they provide persuasive comparative standards. They point towards practical safeguards such as early dismissal mechanisms, costs protection, penalties for abusive claimants, protection of journalists and human rights defenders, and judicial recognition that public participation on matters of public interest deserves heightened protection.

In Zimbabwe, the relevance of SLAPPs is growing as journalists, community leaders, digital activists, human rights defenders and CSOs increasingly expose corruption, environmental harm, corporate abuse, public procurement irregularities, electoral concerns and maladministration through online platforms. Digital publication has amplified both the reach of public interest speech and the risks of retaliation. Powerful actors may respond not only through criminal complaints or political pressure, but also through civil litigation designed to intimidate critics. This compendium is therefore important because it helps lawyers identify when a claim is a legitimate vindication of reputation or privacy, and when it is an abuse of process designed to suppress democratic participation.

1.7 Usefulness of the Compendium to Lawyers, CSOs and Human Rights Defenders

The jurisprudence assembled in this compendium shows that courts are already grappling with these tensions. Zimbabwean cases on freedom of expression,[17] online media regulation, access to information, internet shutdowns, privacy, constitutional applications, locus standi and public interest litigation provide the building blocks for a stronger digital rights litigation strategy. The compendium also draws from comparative and regional jurisprudence to fill gaps where Zimbabwean case law is still developing. For example, the cases discussed in the draft

14. OHCHR, The Impact of SLAPPs on Human Rights and How to Respond, 29 April 2024.
15. Council of Europe, Recommendation CM/Rec(2024)2 on countering the use of strategic lawsuits against public participation, adopted 5 April 2024.
16. Directive (EU) 2024/1069 on protecting persons who engage in public participation from manifestly unfounded claims or abusive court proceedings (Strategic Lawsuits Against Public Participation).
17. This compendium, chapters on constitutional applications, direct access, freedom of expression, digital freedoms, access to information, data privacy and data protection.

demonstrate the importance of legality in internet shutdowns, lawful regulation of online media actors, the constitutional value of public interest reporting, the limits of defamation suits by public bodies, the procedural requirements for constitutional litigation, and the need to balance privacy against access to information and freedom of expression.

This compendium is therefore intended to serve both as a legal research tool and as a strategic litigation resource. For human rights lawyers and public interest litigators, it provides authorities that can be used to frame constitutional claims, resist overbroad restrictions, challenge unlawful surveillance, defend journalists and activists, and argue for remedies that protect democratic accountability. For CSOs, it provides a practical map of legal principles that can inform advocacy, policy engagement, training of communities, and rapid response to threats against civic space. For journalists, bloggers, online content creators and human rights defenders, it clarifies the rights and protections available when they report on matters of public interest. For courts and regulators, it highlights the need to interpret existing laws consistently with constitutional values and international human rights standards.

The usefulness of the compendium lies in its ability to connect doctrine with practice. Digital rights violations often occur quickly: an internet shutdown is ordered, a journalist is arrested, a social media user is prosecuted, a CSO is denied information, a whistle-blower is exposed, a data breach occurs, or a powerful actor files a defamation suit to silence criticism. In such moments, lawyers require accessible, well-organised and persuasive authorities. This compendium provides that foundation. It assists practitioners to identify the correct cause of action, determine standing, select the appropriate forum, plead constitutional issues properly, rely on international and regional standards, and anticipate procedural objections such as mootness, exhaustion of remedies, non-joinder, lack of jurisdiction or failure to establish a constitutional matter.

Ultimately, this compendium is premised on the idea that digital rights are democratic rights. Freedom of expression protects the right to speak; access to information protects the right to know; privacy and data protection protect the right to think, communicate and organise without arbitrary intrusion; the right to erasure protects dignity against disproportionate digital permanence; and anti-SLAPP principles protect the right to participate in public affairs without fear of abusive litigation. Together, these rights form the legal infrastructure of an open, accountable and democratic society. In Zimbabwe, where constitutional democracy continues to be shaped through litigation, advocacy and civic engagement, this compendium provides a timely and necessary resource for defending digital freedoms and strengthening public interest litigation.

CHAPTER 02

Constitutional Applications, Direct Access and Locus Standi

This chapter sets out the procedural foundations for digital rights and public interest litigation in Zimbabwe. Before courts can determine the substance of claims concerning freedom of expression, privacy, access to information or digital surveillance, litigants must satisfy threshold requirements relating to standing, jurisdiction, direct access, constitutional referral and the existence of a genuine constitutional matter. The cases discussed below are therefore included not for their digital-rights facts alone, but because they guide practitioners on how to properly frame constitutional claims, select the appropriate forum, anticipate procedural objections and avoid converting ordinary disputes into constitutional litigation without a clear rights-based foundation.

In **Mudzuru v Minister of Justice, Legal and Parliamentary Affairs CCZ 12/15**[18]**,** the Constitutional Court dealt extensively with the issue of locus standi and public interest litigation under section 85(1) of the Constitution. Locus standi refers to the legal right or capacity of a person to bring a matter before the court. The Court explained that section 85(1) liberalised the traditional narrow approach to standing and allows a broader range of persons to approach the courts in constitutional matters involving the infringement of fundamental rights. Under section 85(1), standing may arise where a person acts in their own interests, on behalf of another person who cannot act for themselves, as a member or in the interests of a group or class, in the public interest, or as an association acting in the interests of its members. The Court stated that under section 85(1)(a), a person acting in their own interests must show that their own rights or legally protected interests have been directly affected by the alleged infringement. The infringement must relate either directly to the person or indirectly affect their interests through harm arising from the violation of another person's rights. The Court described this as the traditional approach to locus standi, where a litigant must have a direct relationship with the cause of action.

The applicants in Mudzuru were found not to have standing under section 85(1)(a) because they were no longer children and could not show that their own interests were directly affected by the continued existence of child marriage laws. However, the Court held that they had standing under section 85(1)(d) because they were acting in the public interest. The Court explained that public interest litigation exists to ensure that constitutional rights, especially those affecting vulnerable or disadvantaged groups, are protected even where the victims themselves cannot easily approach the courts. Children were regarded as a vulnerable class deserving special constitutional protection. The Court stated that section 85(1)(d) is based on the broadest conception of standing and is intended to ensure effective protection of public interests adversely affected by constitutional violations.

---

18. Mudzuru v Minister of Justice, Legal and Parliamentary Affairs CCZ 12/15, Constitutional Court of Zimbabwe, on locus standi and public interest litigation under s 85 of the Constitution.

The Court emphasised that a person suing in the public interest does not need to show personal benefit or direct injury. Instead, the litigant must demonstrate that the litigation genuinely seeks to protect a broader public interest rather than private, personal, political, or ulterior motives.

The Court warned that public interest litigation should not be abused by "busybodies" or meddlesome interlopers seeking publicity or pursuing private agendas disguised as constitutional litigation. To determine whether a litigant is genuinely acting in the public interest, the Court adopted factors from comparative constitutional jurisprudence, including whether there is another reasonable and effective manner to bring the challenge, the nature of the relief sought, the extent to which the relief has general application, the vulnerability of the affected persons, the importance of the right being protected, and the consequences of the alleged infringement.

The Court further explained that public interest litigation is especially important where vulnerable persons such as children, the poor, marginalised groups, or disadvantaged communities are unable to approach the courts themselves because of poverty, disability, lack of knowledge, or social disadvantage. The Court stressed that section 85(1)(d) was introduced to widen access to justice and to ensure effective enforcement of constitutional rights and the rule of law. The Court also held that where legislation is alleged to be unconstitutional, a litigant acting in the public interest does not need to identify specific victims whose rights have already been infringed. The existence of legislation inconsistent with the Constitution itself gives rise to constitutional invalidity, and a public interest litigant may challenge such legislation to vindicate the Constitution and protect society generally.

In the end, the Court concluded that the applicants were acting altruistically and genuinely in the public interest by seeking protection for girl children subjected to early marriages. The applicants had no personal gain to derive from the litigation and were motivated by the need to protect vulnerable children and uphold constitutional supremacy. The Court therefore recognised their locus standi under section 85(1)(d) **and proceeded to determine the constitutional validity of child marriage laws in Zimbabwe.**

Joseph Mwoyounotsva v ZINWA CCZ 9/20

The case of Joseph Mwoyounotsva v ZINWA CCZ 9/20[19] is an important authority on constitutional applications, direct access to the Constitutional Court, and the meaning of a "question of law" in Zimbabwean jurisprudence. The judgment is particularly significant for public interest litigators and human rights lawyers because it clarifies the limits of constitutional litigation, the exceptional nature of direct access applications, and the distinction between constitutional matters and ordinary disputes disguised as constitutional claims. The applicant approached the Constitutional Court in terms of s 167(5)(a) of the Constitution seeking direct access on the basis that the Supreme Court had violated his constitutional rights, particularly the right to equal protection of the law under s 56(1) of the Constitution. The Constitutional Court, however, dismissed the application and reaffirmed that direct access is an extraordinary procedure which is granted only in deserving cases where strict procedural and substantive requirements are satisfied.

19. Joseph Mwoyounotsva v Zimbabwe National Water Authority CCZ 9/20, Constitutional Court of Zimbabwe, on direct access, constitutional matters and questions of law.

The Court emphasised that compliance with Rule 21 of the Constitutional Court Rules is not a mere technicality. An applicant must show that it is in the interests of justice for the Constitutional Court to hear the matter directly. The Court relied on earlier jurisprudence such as **Liberal Democrats v President of Zimbabwe & Ors**[20] where it was stated that direct access is not a routine procedure but an exceptional procedure. The judgment demonstrates the Constitutional Court's concern that if every dissatisfied litigant were allowed to approach it directly, the Court would become both a court of first and last instance, undermining the judicial hierarchy and depriving litigants of the benefit of prior judicial consideration by lower courts. For strategic litigators, this case is an important reminder that constitutional arguments should be raised and developed from the earliest stages of litigation rather than after losing in the ordinary courts.

One of the most significant contributions of this case is its discussion of what constitutes a constitutional matter. The Court reiterated that in terms of s 332 of the Constitution, a constitutional matter is one involving the interpretation, protection, or enforcement of the Constitution. Relying on Moyo v Chacha, the Court stressed that not every legal dispute or judicial error becomes a constitutional issue merely because constitutional language is invoked. The Constitutional Court only has jurisdiction where there is a genuine constitutional question. This is particularly important for public interest lawyers who often seek to elevate labour, administrative, electoral, or governance disputes into constitutional litigation. The case warns litigants that constitutional litigation requires substantive constitutional issues and not mere dissatisfaction with the outcome of ordinary proceedings.

The judgment is also important for its detailed explanation of the meaning of a "question of law." In terms of s 92F(1) of the Labour Act, appeals from the Labour Court to the Supreme Court lie only on questions of law. The applicant argued that the Supreme Court had improperly treated factual issues as questions of law. The Constitutional Court rejected this argument and confirmed that, in certain circumstances, a gross misdirection on the facts may amount to a question of law. The Court relied on authorities such as RBZ v Granger, Zimbabwe Open University v Ndekwere, and Zvokusekwa v Bikita Rural District Council, which established that where a factual finding is so unreasonable, irrational, or unsupported by evidence that no sensible tribunal could have reached it, the issue transcends a mere factual dispute and becomes a legal question. This principle is highly valuable for strategic litigators because many statutes limit appeals to "questions of law." The case therefore provides a pathway for challenging irrational findings by lower tribunals and administrative bodies by framing them as legal errors arising from gross factual misdirection.

The case further clarifies the circumstances under which judicial decisions themselves may be challenged as unconstitutional. The Court accepted that judicial conduct may violate constitutional rights where the judicial process itself is fundamentally unfair or unlawful. However, the Court stressed that the Constitution guarantees fair judicial protection, not infallible judicial outcomes. Judicial officers may make mistakes, but not every mistake amounts to a constitutional violation. What must be shown is that the judicial officer failed to comply with the legal standards governing the proceedings to such an extent that the litigant was denied constitutional protection. This distinction is crucial for public interest litigators seeking to challenge judicial

20. CCZ 7/18

conduct in politically sensitive cases, electoral disputes, or cases involving abuse of process. The case suggests that constitutional review may succeed where there is evidence of procedural unfairness, bias, arbitrariness, denial of a fair hearing, or disregard of mandatory legal standards. However, mere disagreement with the reasoning or conclusions of a court is insufficient.

Another major theme in the judgment is the principle of finality of Supreme Court decisions in non-constitutional matters. The Court strongly defended the constitutional position that decisions of the Supreme Court in non-constitutional disputes are final and binding. Relying on authorities such as **Lytton Investments v Standard Chartered Bank Zimbabwe Ltd and Williams v Msipha,** the Court held that a litigant cannot simply re-open litigation through constitutional proceedings because they are dissatisfied with the Supreme Court's conclusions. The Court stated that the finality of Supreme Court decisions is itself part of the constitutional protection of the law. This aspect of the judgment has profound implications for strategic litigation because it means that constitutional dimensions of a dispute must be identified and pleaded early. Litigants who fail to constitutionalise issues at the appropriate stage may later find themselves procedurally barred from constitutional review.

The Court was also critical of attempts to disguise ordinary appeals as constitutional applications. It observed that the applicant's case was essentially a complaint against the factual and legal findings of the Supreme Court rather than a genuine constitutional grievance. The Court described such applications as attempts by disgruntled litigants to obtain another appeal under the guise of constitutional litigation. This warning is particularly relevant for public interest lawyers because poorly framed constitutional claims may undermine the credibility of strategic litigation and result in dismissal on jurisdictional grounds. The judgment therefore encourages careful constitutional pleading and disciplined litigation strategy.

The case additionally contains important guidance on locus standi and public interest litigation. The applicant attempted to approach the Court both in his personal capacity and in the public interest under s 85(1)(a) and (d) of the Constitution. The Court rejected this approach and reaffirmed the principle from **Mudzuru v Minister of Justice** that litigants should act in one capacity only when approaching the Court. This aspect of the judgment is particularly important for NGOs, activists, and public interest organisations because it highlights the need for clarity regarding standing. Lawyers must carefully determine whether an applicant is litigating personally, on behalf of others, as a class representative, or purely in the public interest. Failure to properly structure standing arguments may defeat an otherwise strong constitutional case.

From a broader constitutional perspective, the judgment reflects the Constitutional Court's cautious approach toward expansive constitutional review. The Court prioritised judicial finality, procedural discipline, and jurisdictional limits over a broader transformative interpretation of constitutional access. Some critics may argue that the decision adopts an overly restrictive approach that limits access to constitutional justice and shields judicial decisions from accountability. Others may contend that the Court was justified in protecting the integrity of the judicial hierarchy and preventing abuse of constitutional litigation procedures. Regardless of one's perspective, the case remains a foundational authority on constitutional jurisdiction, direct access, and the boundaries of strategic litigation in Zimbabwe.

For public interest lawyers and human rights litigators, the practical lessons from the case are clear. Constitutional arguments should be raised from the outset of litigation and not introduced only after adverse judgments have been issued. Litigants seeking constitutional review of judicial decisions must focus on procedural unfairness, irrationality, arbitrariness, or violations of constitutional standards governing adjudication rather than simply asserting that the court reached the wrong conclusion. The case also demonstrates the importance of carefully constructing public interest standing and ensuring that constitutional claims are genuine, well-supported, and connected to identifiable constitutional rights. Ultimately, Joseph Mwoyounotsva v ZINWA is an essential authority for understanding constitutional procedure, appellate jurisdiction, and the limits of constitutional litigation in Zimbabwean law.

Rita Marque Mbatha v Confederation of Zimbabwe Industries & Another CCZ 13/20

The case of Rita Marque Mbatha v Confederation of Zimbabwe Industries and The Sheriff of Zimbabwe CCZ 13/20 is an important authority on direct access to the Constitutional Court, procedural compliance in constitutional litigation, and the principle that constitutional jurisdiction should not be used to interrupt ongoing proceedings in lower courts except in exceptional circumstances. The judgment reinforces the Constitutional Court's restrictive and disciplined approach to direct access applications under s 167(5) of the Constitution and provides important lessons for public interest litigators and human rights lawyers regarding constitutional procedure, jurisdiction, and litigation strategy.

The applicant sought leave for direct access to the Constitutional Court in terms of s 167(5) of the Constitution as read with r 21 of the Constitutional Court Rules. She alleged that her constitutional right to protection of the law under s 56(1) of the Constitution had been violated by a judgment of the High Court. The Constitutional Court was therefore required to determine whether it was in the interests of justice to permit the applicant to bypass ordinary court procedures and approach the Constitutional Court directly. In dismissing the application, the Court reiterated that direct access is an extraordinary remedy which is granted only in exceptional circumstances and where strict procedural and substantive requirements are satisfied.

One of the most important aspects of the judgment is the Court's emphasis on procedural compliance in constitutional litigation. Rule 21(2) requires that an application for direct access be supported by an affidavit setting out the facts upon which the applicant seeks relief. The applicant failed to comply with this requirement and instead attempted to incorporate affidavits and pleadings filed in separate High Court proceedings. The Court criticised this omission and stressed that constitutional litigants must properly set out the factual basis of their claims within the application itself. Although the Court ultimately held that the omission was not fatal because the High Court record adequately disclosed the relevant facts, the judgment nevertheless demonstrates the importance the Constitutional Court places on procedural discipline and proper pleading.

For public interest litigators, this aspect of the case is highly significant because constitutional litigation often involves urgent matters where litigants may be tempted to rely on existing records rather than carefully drafted constitutional pleadings.

21. Rita Marque Mbatha v Confederation of Zimbabwe Industries and The Sheriff of Zimbabwe CCZ 13/20, Constitutional Court of Zimbabwe, on direct access and procedural discipline in constitutional litigation.

The judgment makes clear that constitutional applications must independently satisfy the procedural requirements prescribed by the Rules. Strategic litigators must therefore ensure that founding affidavits are comprehensive, properly structured, and specifically tailored to constitutional relief sought. Failure to comply with procedural rules may result in dismissal of otherwise potentially meritorious claims.

The judgment also provides important guidance on the meaning and purpose of direct access to the Constitutional Court. The Court reiterated that it is a specialised court with limited jurisdiction under s 167(1) of the Constitution and that it only determines constitutional matters and issues connected with constitutional matters. Direct access is therefore not an ordinary procedural shortcut but a carefully controlled jurisdictional mechanism. The Court relied heavily on the principle articulated by Currie and de Waal in The Bill of Rights Handbook that direct access should remain exceptional because unrestricted constitutional access would burden the Constitutional Court with factual disputes, academic questions, and matters that ought first to be ventilated in lower courts. The Court also stressed that it is generally undesirable for a court to sit as both a court of first and final instance because litigants would be deprived of appeal opportunities and the benefit of lower court reasoning.

This reasoning has major implications for strategic public interest litigation. The case reinforces the need for litigants to build constitutional arguments progressively through the judicial hierarchy rather than attempting to approach the Constitutional Court prematurely. Public interest lawyers must therefore think strategically about forum selection and procedural sequencing. Constitutional arguments should ordinarily be raised in lower courts first so that a proper factual and legal record is developed before the matter reaches the apex court. The judgment discourages litigants from using direct access as a mechanism for avoiding ordinary litigation procedures or correcting procedural mistakes made earlier in the litigation process.
Another important principle established by the case is that the interests of justice inquiry involves a number of considerations, including prospects of success, availability of alternative remedies, and the existence of factual disputes. The Court relied on r 21(8) and its earlier decision in Lytton Investments v Standard Chartered Bank Zimbabwe Ltd to emphasise that an applicant must not only demonstrate why direct access is necessary but must also show that the substantive constitutional application has prospects of success. This is particularly important for strategic litigators because it means that constitutional applications must be substantively persuasive at the leave stage itself. Applicants must therefore carefully articulate both the constitutional violation and the reasons why the Constitutional Court should intervene directly.

The Court further held that the application was ill-conceived because proceedings between the parties were still pending in the High Court. This aspect of the judgment is extremely important in constitutional litigation because it reaffirms the long-standing common law principle that superior courts should be reluctant to interfere with ongoing proceedings in lower courts except in exceptional circumstances. The Court relied on Chihava v Provincial Magistrate Mapfumo and the South African case of Wahlhaus v Additional Magistrate, Johannesburg in holding that intervention in pending proceedings is justified only where grave injustice would otherwise result or where justice cannot be attained through ordinary procedures.

This principle has substantial implications for public interest litigation, especially in politically sensitive cases, criminal prosecutions, electoral disputes, or cases involving human rights violations. Litigants often seek urgent constitutional intervention while proceedings are still underway in lower courts. This case makes clear that the Constitutional Court will generally refuse to intervene unless there are truly exceptional circumstances demonstrating imminent and irreparable injustice. Strategic litigators must therefore carefully assess whether constitutional intervention is genuinely necessary or whether adequate remedies remain available through ordinary court procedures.

The Court also relied on South African constitutional jurisprudence, particularly Bruce v Fleecytex Johannesburg CC, to emphasise that direct access should not be used to avoid the consequences of earlier procedural omissions or to bypass normal appeal procedures. The Constitutional Court warned against litigants attempting to transform ordinary procedural grievances into constitutional claims in order to obtain expedited access to the apex court. This aspect of the judgment reflects broader judicial concerns regarding abuse of constitutional litigation procedures and preservation of judicial hierarchy.

From a strategic litigation perspective, the case demonstrates the Constitutional Court's commitment to judicial restraint and procedural orderliness. The Court sought to preserve the integrity of ordinary litigation processes while ensuring that constitutional jurisdiction remains reserved for genuine constitutional controversies requiring urgent and exceptional intervention. Public interest litigators should therefore understand that constitutional litigation is not merely about raising constitutional language but about satisfying strict jurisdictional and procedural thresholds.

The judgment may, however, also be criticised from a transformative constitutionalism perspective. Critics may argue that the Court's restrictive approach to direct access creates barriers to constitutional justice, particularly for vulnerable litigants who may lack resources to pursue lengthy litigation through multiple court levels. Others may contend that excessive procedural formalism risks undermining substantive constitutional protection by prioritising technical compliance over access to justice. Nonetheless, the Court appears motivated by concerns about maintaining judicial efficiency, preventing abuse of constitutional procedures, and protecting the Constitutional Court from becoming overwhelmed by ordinary disputes framed as constitutional matters.

For public interest and human rights lawyers, the practical lessons from this case are significant. Constitutional litigants must ensure strict compliance with procedural requirements under the Constitutional Court Rules, particularly regarding founding affidavits and the factual basis of constitutional claims. Applicants seeking direct access must clearly demonstrate exceptional circumstances, prospects of success, and the absence of adequate alternative remedies. Lawyers should avoid approaching the Constitutional Court while proceedings remain pending in lower courts unless there is clear evidence that grave injustice will occur without immediate intervention. The case also highlights the importance of raising constitutional issues at the earliest stages of litigation and developing a strong constitutional record within lower courts before seeking access to the Constitutional Court.

Ultimately, Rita Marque Mbatha v Confederation of Zimbabwe Industries and The Sheriff of Zimbabwe is an important authority on constitutional procedure, direct access jurisdiction, and judicial restraint in Zimbabwean constitutional law. It provides valuable guidance for strategic litigators regarding the careful structuring of constitutional claims, respect for procedural hierarchy, and the exceptional nature of direct constitutional access.

Alistair Michael Fletcher v Minister of Lands, Agriculture, Fisheries, Water and Rural Resettlement & Others[22] CCZ 7/24

Key issue: What constitutes a constitutional matter for purposes of an appeal to the Constitutional Court, and what requirements must be satisfied in an application for leave to appeal.

Legal Principle

The Constitutional Court reaffirmed that its jurisdiction is limited to constitutional matters only. A litigant seeking leave to appeal to the Constitutional Court must clearly demonstrate that the intended appeal raises a genuine constitutional issue, not merely an ordinary legal, factual, procedural, or evidentiary dispute dressed in constitutional language.

A constitutional matter is one involving the interpretation, protection or enforcement of the Constitution, as contemplated by section 332 of the Constitution. The constitutional issue must have been properly raised and determined in the lower court. It is not enough for a party to mention constitutional provisions after the fact or to frame dissatisfaction with a lower court's decision as a constitutional complaint.

Requirements for Leave to Appeal to the Constitutional Court

The Court restated the established requirements for leave to appeal. An applicant must show that:

- The intended appeal raises a constitutional matter that is clearly and concisely set out.
- The constitutional matter arose from, and was determined in, the decision of the lower court.
- The intended appeal enjoys prospects of success.
- The appeal is in the interests of justice.

The Court emphasised that prospects of success require more than an arguable case. The applicant must show that, on appeal, the Constitutional Court is likely to reverse the decision of the lower court or materially alter the order granted by that court.

22. Alistair Michael Fletcher v Minister of Lands, Agriculture, Fisheries, Water and Rural Resettlement & Others CCZ 7/24, Constitutional Court of Zimbabwe, on leave to appeal and the definition of a constitutional matter.

Meaning of a Constitutional Matter

The Court relied on earlier authorities including **Cold Chain (Pvt) Ltd t/a Sea Harvest v Makoni[23], Chombo v National Prosecuting Authority, Bere v Judicial Service Commission**, **Lytton Investments v Standard Chartered Bank Zimbabwe Ltd, and Mudyavanhu v Saruchera**. These cases establish that a constitutional matter exists only where the dispute requires the court to interpret, protect, or enforce a provision of the Constitution.

The mere fact that a party alleges unfairness, illegality, procedural irregularity, or error by a lower court does not automatically create a constitutional issue. The lower court must have been required to determine a genuine constitutional question.

Jurisdictional Significance

The case confirms that the Constitutional Court is a specialised court and not a general appellate court. It does not hear appeals on non-constitutional matters. A decision of a subordinate court on a non-constitutional issue is not appealable to the Constitutional Court because the Court lacks jurisdiction over such matters.

Rule Emerging from the Case

A litigant cannot invoke the jurisdiction of the Constitutional Court simply by labelling a dispute as constitutional. The constitutional issue must be genuine, clearly pleaded, properly raised before the lower court, and necessary for the resolution of the dispute. Where the dispute is essentially factual, procedural, statutory, contractual, or evidentiary, the Constitutional Court will not assume jurisdiction unless the matter directly involves constitutional interpretation, protection, or enforcement.

Importance of the Case

This case is important for strategic litigation because it clarifies the threshold for accessing the Constitutional Court on appeal. It cautions litigants against constitutionalising ordinary disputes and confirms that constitutional appeals must be carefully framed from the earliest stage of litigation. It also reinforces the need for lawyers to identify and plead constitutional issues clearly before the lower courts if they intend to pursue a constitutional appeal.

23. Cold Chain (Pvt) Ltd t/a Sea Harvest v Makoni 2017 (1) ZLR 14 (CC), on the requirement that a constitutional matter involve interpretation, protection or enforcement of the Constitution.

CHAPTER 03

Freedom of Expression and Digital Freedoms

Zimbabwean and comparative jurisprudence has played an important role in shaping the protection of freedom of expression, media freedom, and public participation in democratic discourse, particularly in the digital era where communication increasingly takes place through online platforms and social media. The courts have generally recognised that freedom of expression is a foundational constitutional right necessary for accountability, democratic governance, and public scrutiny of both State and non-State actors.

In **Chimakire & Ors v The Attorney-General of Zimbabwe CCZ 6/14,**[24] the Constitutional Court declared section 31(a)(iii) of the Criminal Law Code unconstitutional and null and void. The impugned provision criminalised the publication of false statements wholly or materially false with the intention of undermining public confidence in law enforcement agencies, the Prison Service, or the Defence Forces of Zimbabwe. The Constitutional Court held that the provision violated section 20(1) of the former Constitution, which protected freedom of expression. The Court found that the restriction imposed by the provision was not reasonably justifiable in a democratic society because it was overbroad, disproportionate, and had a chilling effect on legitimate speech and public debate. The Court also took issue with the severity of the penalty, which provided for imprisonment of up to twenty years. The practical effect of the judgment is that prosecutions can no longer lawfully be pursued under section 31(a)(iii) as it currently stands. Although the case was decided under the pre-2013 Constitution, the same reasoning would equally apply under section 61 of the 2013 Constitution, which expressly protects freedom of expression and freedom of the media. The judgment is particularly important for digital freedoms because it protects citizens, journalists, bloggers, activists, and social media users from vague and excessive criminal sanctions targeting criticism of public institutions. The reasoning in Chimakire also casts doubt on the constitutionality of other broadly worded offences within section 31 of the Criminal Law Code.

In **Thembi-Mahanyele v Mail and Guardian & Another 2004 (6) SA 329 (SCA),**[25] the South African Supreme Court of Appeal reaffirmed the principle that the media plays an essential role in investigating and exposing wrongdoing in both the public and private sectors. The Court recognised that democratic accountability requires the press to be given sufficient latitude to report on matters of public interest, particularly concerning public officials and allegations of corruption. The Court accepted that factual inaccuracies may occur in journalism and held that errors of fact should be tolerated where the publication was made reasonably, justifiably, and in the public interest, based on a reasonable belief in the truth of the information published. The case underscores the constitutional value of political expression and investigative journalism in ensuring that public officials remain accountable to society. The decision has relevance for digital media platforms and online journalism because it recognises that public interest reporting should

24. Chimakire & Ors v Attorney-General of Zimbabwe CCZ 6/14, Constitutional Court of Zimbabwe, declaring s 31(a)(iii) of the Criminal Law Code unconstitutional under the former Constitution.
25. Thembi-Mahanyele v Mail & Guardian Ltd and Another 2004 (6) SA 329 (SCA), on public interest reporting, reasonable publication and democratic accountability.

not be suppressed merely because errors later emerge, provided that the reporting was responsibly undertaken. Similar reasoning was also reflected in Zillie v Johnson & Another 1984 (2) SA 186 (W).

In **Mushunje v Zimbabwe Newspapers HH 47/17,**[26] the High Court adopted an approach drawn from United States constitutional jurisprudence concerning defamation claims brought by public figures. The Court suggested that a public figure could only succeed in a defamation claim if he or she proved that the defamatory statement was published with "actual malice" or with reckless disregard as to whether it was false. Under the American standard, public figures rarely succeed in defamation claims because the burden of proving actual malice is exceptionally high. This approach has not traditionally formed part of Zimbabwean law and has been criticised for affording inadequate protection to the reputations of public figures. While democratic societies should permit robust criticism of public officials and institutions, the adoption of the American approach risks insulating irresponsible and malicious reporting from accountability. The judgment therefore raises important questions about the balance between freedom of expression and protection of reputation in the digital age, particularly in the context of online publications and social media commentary where harmful statements can spread rapidly and widely.

In **PTC v Modus Publications (Pvt) Ltd 1997 (2) ZLR 492 (S)**[27], the Supreme Court considered whether a State-owned corporation could sue a newspaper for defamation. The Posts and Telecommunications Corporation, a statutory body, sought damages for allegedly defamatory statements published against it. The Court held that organs of State do not have locus standi to sue for defamation because allowing such actions would undermine freedom of expression and democratic accountability. The Court reasoned that State institutions must remain open to public criticism and scrutiny. It emphasised that government bodies should not use public funds to silence criticism through defamation litigation. Instead, their remedy lies in political engagement and public response rather than litigation designed to suppress criticism. The Court nevertheless recognised that State bodies are not left without recourse. Where false statements cause actual economic harm, a State body may sue for injurious falsehood or malicious falsehood, but in such cases the burden rests on the State body to prove falsity and resulting loss. The Court further observed that it would be undesirable to create a rigid definition of which entities qualify as organs of State because governmental structures continue to evolve. Instead, factors such as governmental control, financial autonomy, public functions, monopoly status, and the provision of essential public services should be considered. The judgment remains highly significant for civil society organisations, journalists, and digital activists because it protects criticism of public institutions and limits the ability of State entities to weaponise defamation law against critics.

The position adopted in **PTC v Modus Publications** was recently revisited in **Rusape Town Council v Takudzwa Noel Mwashaenyi & Sheriff of the High Court N.O HCMTC 70/25; HCMTJ 39/25**[28]. In this case, the respondent allegedly circulated social media posts accusing the local authority of tender impropriety and corruption. The Court considered whether a local authority possesses a reputation capable of protection through defamation proceedings. In doing so, it referred to the **South African decision in Bitou Municipality and Another v Booysen and Another (2011) ZAWCHC**

26. Mushunje v Zimbabwe Newspapers (1980) Ltd HH 47/17, High Court of Zimbabwe, discussing public figures, actual malice and defamation in Zimbabwean law.
27. Posts and Telecommunications Corporation v Modus Publications (Pvt) Ltd 1997 (2) ZLR 492 (S), on State bodies, defamation and public criticism.
28. Rusape Town Council v Takudzwa Noel Mwashaenyi & Sheriff of the High Court N.O. HCMTC 70/25; HCMTJ 39/25, on defamation claims by local authorities and public criticism on social media.

52, where the Court emphasised that democratically elected governmental bodies must remain open to uninhibited public criticism. The Court reiterated the principle that public bodies should generally not sue for defamation because such actions threaten democratic discourse and freedom of expression.

However, the Court also reaffirmed that public bodies may still pursue remedies for injurious falsehood where false statements result in measurable economic loss. The judgment is particularly relevant in the digital era because allegations concerning public corruption, maladministration, and abuse of office are now frequently disseminated through social media platforms. The case therefore illustrates the ongoing tension between protecting democratic debate online and safeguarding institutions from demonstrably false statements causing tangible harm.

In **Dudzai Mureyi v Health Professions Authority of Zimbabwe and Others HH 823/17 HC 8602/16,** [29] the High Court addressed the intersection between technology, access to information, healthcare rights, and administrative justice. The applicant, a pharmacist, sought to establish a digital database that would enable members of the public to locate healthcare providers, identify the availability of medicines, and access information regarding registered drugs and medical services in a more efficient and cost-effective manner. The regulatory authorities refused to approve the initiative on the basis that it allegedly constituted unlawful advertising and fell outside the statutory framework governing health institutions.

The Court held that the respondents acted unconstitutionally by relying on an unduly narrow and restrictive interpretation of their enabling legislation while ignoring their constitutional obligations under section 44 of the Constitution to respect, protect, promote, and fulfil constitutional rights and freedoms. The Court criticised the respondents for their "apprehension of modern technology" and for creating unnecessary barriers to innovation and private initiative within the healthcare sector. It found that the proposed database did not amount to advertising but rather enhanced the dissemination of information already routinely shared by healthcare professionals. The Court further held that the concept of a "Health Institution" should be interpreted broadly to accommodate technological developments capable of improving public access to healthcare information and services. The judgment is important in the context of digital rights because it recognises that technology-driven platforms facilitating public access to information are constitutionally protected and that regulatory frameworks must evolve to accommodate innovation. The case also reinforced the principles of administrative justice under section 68 of the Constitution by emphasising that administrative authorities must provide lawful, reasonable, and constitutionally compliant decisions.

In **Zimbabwe Lawyers for Human Rights v Minister of State, National Security**[30], the High Court considered the legality of the nationwide internet shutdown imposed during the January 2019 stay-away organised by the Zimbabwe Congress of Trade Unions. Following widespread protests and arrests, internet and social media access, including WhatsApp and Facebook, were disrupted throughout Zimbabwe after the Minister of State for National Security purportedly issued directives under the Interception of Communications Act. Telecommunications providers

29. Dudzai Mureyi v Health Professions Authority of Zimbabwe and Others HH 823/17, HC 8602/16, on technology, access to health information and administrative justice.
30. Zimbabwe Lawyers for Human Rights and Media Institute of Southern Africa-Zimbabwe v Minister of State for National Security and Others, High Court of Zimbabwe, January 2019 internet shutdown litigation.

confirmed publicly that they had been compelled to suspend services pursuant to governmental instructions. The shutdown prompted urgent legal proceedings by the Zimbabwe Lawyers for Human Rights and the Media Institute of Southern Africa. The applicants argued that the shutdown constituted an unjustifiable limitation on freedom of expression protected under section 61 of the Constitution and that it severely affected ordinary citizens, businesses, communication, and access to information. The Court ultimately found in favour of the applicants on the issue of legality, holding that the Interception of Communications Act vested the relevant powers exclusively in the President and not in the Minister. Consequently, the Minister lacked authority to order the internet shutdown. The Court therefore set aside the directive and ordered telecommunications companies to restore full and unrestricted internet access. Although the judgment did not declare internet shutdowns themselves unconstitutional, it represented an important affirmation of legality, constitutionalism, and digital freedoms. The decision highlighted the importance of internet access as a modern platform for communication, expression, commerce, and civic participation. At the same time, the judgment left unresolved the broader constitutional question of whether the President himself may lawfully impose internet shutdowns consistent with constitutional rights and democratic standards.

In **Zimbabwe Online Content Creators Trust (ZOCC) v Zimbabwe Media Commission HH 359/20**[31], the High Court dealt directly with the recognition and regulation of online media practitioners in Zimbabwe. The applicant, a trust representing online content creators, bloggers, social media practitioners, online editors, and digital journalists, challenged the Zimbabwe Media Commission's decision to introduce new categories of media accreditation through a press statement. The Commission had expanded accreditation categories beyond the two categories recognised under the Access to Information and Protection of Privacy Act, purportedly in response to developments in digital media.

The applicant argued that the Commission's actions violated sections 61 and 62 of the Constitution, which protect freedom of expression, media freedom, and access to information. It further contended that the Commission acted without proper legal authority, stakeholder consultation, or parliamentary approval. The Court agreed with the applicant and held that the Commission had acted ultra vires the statute. Applying the principle of constitutional avoidance, the Court resolved the matter through statutory interpretation rather than direct constitutional adjudication. It held that the legislation only recognised local and foreign journalists as accreditation categories and that the Commission could not create additional categories through administrative action or press statements. The Court emphasised that if the law was inadequate to address developments in digital media, the proper course was legislative reform through Parliament rather than unilateral action by the Commission.

The judgment is highly significant for digital rights and freedom of expression because it affirmed that online journalists, bloggers, content creators, and digital media practitioners are entitled to equal legal recognition and protection. The Court prevented the use of administrative accreditation systems as a mechanism to arbitrarily exclude or discriminate against digital media actors. In doing so, it reinforced the constitutional principle that media regulation must remain lawful, transparent, and consistent with freedom of expression in the digital age.

31. Zimbabwe Online Content Creators Trust v Zimbabwe Media Commission HH 359/20, on online media accreditation, legality and freedom of expression.

In **Joshua Chisa Mbele v The Director of Public Prosecutions & The Attorney General [2025]** [32] MWHC (Constitutional Referral No. 2 of 2024), the Malawi Constitutional Court made a landmark contribution to freedom of expression and digital rights in Africa by striking down section 200 of the Penal Code and effectively decriminalising defamation. The Court held that criminal sanctions for defamatory speech constituted an unjustifiable limitation on freedom of expression because civil remedies were sufficient to protect reputation. The judgment recognised that criminal defamation laws have a chilling effect on public debate, journalism, civic participation, and online speech.

The Court further held that restrictions on digital expression must satisfy the constitutional standards of legality, necessity, and proportionality. This approach strengthened protections for online civic engagement and aligned with emerging regional standards developed by the African Commission on Human and Peoples' Rights concerning freedom of expression and information integrity online. The decision has strong parallels with Zimbabwean constitutional jurisprudence, particularly Chimakire & Others v Attorney-General of Zimbabwe CCZ 6/14, where the Constitutional Court invalidated criminal provisions restricting expression on the basis that they were disproportionate and inconsistent with democratic freedoms. Together, these judgments demonstrate a growing constitutional trend within Africa toward stronger protection of digital rights, online expression, media freedom, and open democratic discourse

32. Joshua Chisa Mbele v Director of Public Prosecutions & Attorney General, Constitutional Referral No. 2 of 2024, High Court of Malawi, on criminal defamation and freedom of expression.

CHAPTER 04

Constitutional Framework

The right of access to information is constitutionally protected under section 62 of the Constitution of Zimbabwe Amendment (No. 20) Act, 2013. Section 62(1) guarantees every Zimbabwean citizen and permanent resident, including the media, the right to access information held by the State or by institutions and agencies of government at every level, where such information is required in the interests of public accountability. Section 62(2) further extends this right to information held by any person, including the State, where the information is required for the exercise or protection of a right.

The constitutional protection of access to information is closely linked to freedom of expression and media freedom under section 61 of the Constitution. In practice, access to information enables journalists, civil society organisations, researchers, and citizens to hold public institutions accountable, expose corruption and maladministration, and meaningfully participate in democratic governance.

However, section 62(4) of the Constitution permits legislation limiting access to information in certain circumstances. Such limitations may only be imposed where they are fair, reasonable, necessary and justifiable in a democratic society based on openness, justice, human dignity, equality and freedom. Despite this constitutional framework, the implementation of access to information rights in Zimbabwe remains constrained by restrictive legislation, particularly provisions inherited from the Access to Information and Protection of Privacy Act [Chapter 10:27] ("AIPPA") and the Official Secrets Act [Chapter 11:09]. Many of these provisions are overly broad and potentially inconsistent with constitutional standards.

The courts in Zimbabwe and comparative jurisdictions have increasingly recognised that access to information is fundamental to constitutional democracy, transparency, accountability, and the enjoyment of other rights. The cases discussed in this chapter illustrate the evolving jurisprudence on access to information and the obligations placed upon public authorities when limiting access.

President of the Republic of South Africa and Others v M & G Media Ltd (CCT 03/11) [2011] ZACC 32[33]; 2012 (2) BCLR 181 (CC); 2012 (2) SA 50 (CC)

In 2002, former South African President Thabo Mbeki dispatched two senior judges to Zimbabwe to investigate and report on legal and constitutional issues surrounding Zimbabwe's presidential election. The judges prepared a report and submitted it to the Presidency. In 2008, M & G Media Limited, the publisher of the Mail & Guardian newspaper, requested access to the report in terms of the Promotion of Access to Information Act 2 of 2000 (PAIA). The Presidency refused access on the

33. President of the Republic of South Africa and Others v M & G Media Ltd (CCT 03/11) [2011] ZACC 32; 2012 (2) SA 50 (CC), on access to State-held information and the burden to justify secrecy.

grounds that the report contained confidential information supplied by another State and that it had been prepared to assist the President in formulating policy. The High Court and the Supreme Court of Appeal ordered disclosure of the report, after which the Presidency appealed to the Constitutional Court.

The Constitutional Court considered whether the Presidency had lawfully refused access to the report, how the State discharges its burden under section 81(3) of PAIA when refusing access to information, and under what circumstances a court may examine a disputed record in camera in terms of section 80 of PAIA. The Court reaffirmed that section 32 of the South African Constitution guarantees the right of access to information held by the State and that PAIA exists to give effect to that constitutional right. It emphasised that disclosure is the rule while secrecy is the exception and held that the State bears the burden of proving, on a balance of probabilities, that a requested record falls within a valid statutory exemption.

The Court rejected the practice of relying on bare assertions or merely repeating statutory language when refusing access to information. It held that the State must provide sufficient evidence to justify non-disclosure and that affidavits filed in support of refusal must demonstrate how the deponent acquired personal knowledge of the facts relied upon. The Court further held that judicial powers under section 80 of PAIA to inspect disputed records in camera must be exercised sparingly and only where it is in the interests of justice. Such powers may be invoked where the State claims that secrecy provisions prevent fuller disclosure, where the requester cannot effectively challenge the refusal without access to the document, where doubts exist regarding the claimed exemption, or where severability of portions of the record is in issue. The matter was ultimately remitted to the High Court for reconsideration after examination of the report in camera.

The judgment is significant because it establishes that disclosure is the default constitutional position and that public bodies must justify secrecy rather than merely assert it. The Court affirmed that transparency and accountability are foundational values of constitutional democracy and that access to information is essential for democratic participation and the protection of other rights. The case also confirms that courts retain oversight powers to independently assess whether claims of confidentiality or national security are lawfully justified.
Although the matter was decided in South Africa, it is highly persuasive in Zimbabwe because section 32 of the South African Constitution is materially similar to section 62 of the Constitution of Zimbabwe. The judgment provides important guidance on the obligation of the State to justify restrictions on access to information and reinforces the principle that limitations on constitutional rights must be narrowly construed. It further supports a constitutional culture of justification in which government secrecy must be shown to be lawful, necessary and proportionate rather than automatically presumed.

Blind SA v Minister of Trade, Industry and Competition and Others (CCT 320/21) [2022] ZACC 33[34]; 2023 (2) BCLR 117 (CC); 2022 BIP 518 (CC); [2022] HIPR 204 (CC)

Blind SA, a non-profit organisation advocating for the rights and interests of blind and visually

34. Blind SA v Minister of Trade, Industry and Competition and Others (CCT 320/21) [2022] ZACC 33, on accessible format copies, equality, dignity, education and access to information.

impaired persons, challenged the constitutionality of provisions of the South African Copyright Act 98 of 1978 which required copyright owner authorisation before literary works could be converted into accessible format copies such as braille, audio, large print or digital formats compatible with screen readers. The organisation argued that these restrictions created what is commonly referred to as a "book famine", where only a very small percentage of books globally are available in accessible formats for persons with visual and print disabilities. Evidence before the Court showed that school learners were unable to obtain textbooks in accessible formats, university students could not access prescribed materials, and many visually impaired persons were routinely denied access to information, education and participation in cultural life.

The Constitutional Court was asked to determine whether the Copyright Act unfairly discriminated against persons with visual and print disabilities and infringed their constitutional rights by requiring authorisation before accessible format copies could be produced. The Court also considered whether section 13 of the Act, which permitted regulations relating to reproduction of works, cured the constitutional defect and what remedy would be just and equitable.

The Court held that the requirement of prior authorisation created a stark disparity between persons with disabilities and persons without disabilities in accessing literary works. It found that this amounted to unfair discrimination because copyright legislation could not be applied as though all persons requiring access to literary works were similarly situated when, in reality, persons with visual and print disabilities faced unique barriers. The Court emphasised that substantive equality sometimes requires differential treatment in order to achieve genuinely equal outcomes. Applying identical rules to groups with vastly different circumstances may itself constitute discrimination.

The Court further held that the restrictions violated the dignity of persons with disabilities because access to literature, information and knowledge is closely connected to human development, imagination and self-worth. Denying such access compounded the marginalisation and adversity already experienced by persons with disabilities. The Court also found infringements of the rights to freedom of expression, education and participation in cultural life because the inability to access books and learning materials severely limited the ability of persons with disabilities to receive and impart information, pursue education and engage fully in society.
In considering whether section 13 of the Copyright Act could remedy the defect, the Court observed that the provision only authorised regulations concerning reproduction of works. However, converting works into accessible formats frequently requires adaptation rather than simple reproduction. For example, braille transcription, audio description of images and diagrams, and the conversion of visual materials into accessible formats often involve interpretation and transformation beyond mere copying. The Court concluded that section 13 was insufficient to cure the constitutional defect because it did not adequately accommodate the full range of accessibility measures required by persons with disabilities.

The Court criticised the lengthy delay by Parliament in amending the Copyright Act despite longstanding awareness of the discriminatory consequences of the legislation. It held that intellectual property rights cannot be enforced in a manner that unjustifiably disadvantages

vulnerable groups who have the same need to access literary works as everyone else. The Court emphasised that where rights infringements are urgent and ongoing, courts may grant interim remedies to protect constitutional rights pending legislative reform.

The Constitutional Court confirmed the declaration of constitutional invalidity and held that sections 6 and 7, read together with section 23 of the Copyright Act, were unconstitutional to the extent that they limited access by persons with visual and print disabilities to published literary and artistic works in accessible formats. The Court suspended the declaration of invalidity for twenty-four months to allow Parliament to amend the legislation. During the suspension period, the Court read into the Act a temporary section 13A permitting authorised non-profit entities, beneficiaries and caregivers to make, obtain and distribute accessible format copies without copyright owner authorisation, provided such copies were used exclusively for persons with disabilities and not for profit.

The judgment is significant because it affirms that access to information and literature by persons with disabilities is a constitutional right rather than an act of charity or legislative generosity. It establishes that copyright law must be interpreted and applied in a manner consistent with constitutional guarantees of equality, dignity, education and freedom of expression. The case also demonstrates how intellectual property rights must be balanced against broader constitutional and human rights considerations.

The Court drew extensively from international human rights instruments including the Marrakesh Treaty, the Convention on the Rights of Persons with Disabilities (CRPD), and the International Covenant on Economic, Social and Cultural Rights (ICESCR). The judgment therefore illustrates the important role international law plays in constitutional interpretation within rights-based legal systems.

The decision is particularly relevant to access to information jurisprudence because it recognises that formal access to information is meaningless where structural or technological barriers prevent vulnerable groups from actually obtaining and using information. It reinforces the principle that states have positive obligations to ensure that information is genuinely accessible to all members of society, including persons with disabilities.

Namatai Kwekwedza v Judicial Service Commission & Another[35] HH 140/22

In Namatai Kwekwedza v Judicial Service Commission & Another, the applicant sought to invoke section 62 of the Constitution to compel the Judicial Service Commission (JSC) to disclose detailed information relating to the extension of the Chief Justice's tenure beyond the age of seventy. The request included information on how the JSC arrived at its recommendation, whether meetings were held and resolutions passed, voting records of commissioners, and whether the Chief Justice had declared any conflict of interest. The JSC refused the request, arguing that it had not been made in accordance with the law, that there is no automatic right to access information, and that disclosure would implicate individual rights such as privacy.

35. Namatai Kwekwedza v Judicial Service Commission & Another HH 140/22, High Court of Zimbabwe, on access to information, privacy and mootness.

The High Court affirmed that sections 61 and 62 of the Constitution guarantee both freedom of expression and access to information held by the State where such access is required for public accountability or for the exercise or protection of a right. It further emphasised that section 44 binds all state institutions, including constitutional bodies such as the JSC, to respect, protect and fulfil these rights. However, the Court was equally clear that the right of access to information is not absolute and must be read together with section 57, which protects the right to privacy, and section 86, which permits limitations that are fair, reasonable, necessary and justifiable in a democratic society.

A decisive factor in the case was the doctrine of mootness. The Court found that the underlying issue - the legality of the Chief Justice's tenure - had already been conclusively determined by the Constitutional Court, rendering the dispute academic. Applying principles from cases such as Francis Bere v JSC and Khupe v Parliament, the Court held that where a matter ceases to present a live controversy with practical consequences, the court will decline to adjudicate it. Granting the order sought would therefore have no practical effect, as the issue had already been settled and "the horse had bolted."

The Court also clarified that access to information under section 62 is conditional rather than automatic. A requester must demonstrate that the information is required either for public accountability or for the exercise or protection of a right. In addition, where legislation such as the Freedom of Information Act provides a specific procedure or appeal mechanism, that process must ordinarily be exhausted before approaching the courts for relief. The judgment further recognised that constitutional bodies like the JSC may legitimately withhold certain categories of information, particularly where disclosure would compromise confidentiality of internal deliberations or implicate sensitive personal information, such as medical details or voting records.

This case is important for public interest and strategic litigation because it delineates both the scope and limits of the right to access information. It underscores that while transparency and accountability are constitutional imperatives, courts will balance these against competing rights such as privacy and institutional integrity. It also highlights procedural discipline as a critical requirement in access to information litigation, including the need to demonstrate a live controversy, establish the necessity of the information sought, and exhaust statutory remedies before invoking constitutional relief.

ZANU PF v Zimbabwe Electoral Commission & Another[36] HH 379/18

In ZANU PF v Zimbabwe Electoral Commission & Another, the applicant political party sought to invoke section 62 of the Constitution to compel the Zimbabwe Electoral Commission (ZEC) to disclose detailed information regarding the type, make, and chemical composition of ballot paper intended for use in the 2018 national elections. The request was premised on allegations that the "special paper" used in previous elections contained chemical properties capable of concealing or altering voters' marks in favour of a particular candidate. ZEC refused to disclose the requested information, asserting that it had the exclusive constitutional mandate under section

36. ZANU PF v Zimbabwe Electoral Commission & Another HH 379/18, High Court of Zimbabwe, on access to election information, public accountability and electoral integrity.

239(a) to design, print and distribute ballot papers and that disclosure of the paper's security features would compromise electoral integrity by enabling counterfeiting.

The High Court reaffirmed that section 62 of the Constitution guarantees the right of access to information held by the State or its institutions where such information is required for public accountability or for the exercise or protection of a right, including political rights under section 67. However, the Court emphasised that this right is not absolute and must be read together with section 62(4) and section 86 of the Constitution, which permit limitations in the interests of public security, defence, or professional confidentiality, provided that such limitations are fair, reasonable, necessary, and justifiable in a democratic society.

In applying these principles, the Court held that the applicant had failed to demonstrate that the information sought was "required" either for public accountability or for the exercise or protection of a right. The Court found ZEC's justification for non-disclosure to be compelling, particularly its argument that revealing the technical and security features of ballot paper would create a real risk of counterfeiting and undermine the credibility of the electoral process. It recognised that ballot paper design incorporates both visible and invisible security features that are essential to safeguarding free and fair elections, and that disclosure of such details would defeat their very purpose.

The Court further emphasised that independent constitutional commissions such as ZEC enjoy institutional autonomy, and that section 235(3) of the Constitution prohibits interference with their functions. Decisions relating to the design and procurement of ballot papers fall squarely within ZEC's exclusive administrative domain, and courts will not interfere with such decisions absent clear evidence of irrationality or constitutional violation. The applicant's reliance on "reliable scientific advices" was found to be insufficient, as no concrete or verifiable evidence was presented to substantiate the allegations of electoral manipulation.

The judgment also clarified that speculative or unsubstantiated claims cannot ground a constitutional right to information. A litigant invoking section 62 must provide a factual basis demonstrating both the necessity of the information and the connection to a protected right. The Court stressed that access to information is not a tool for fishing expeditions or for advancing conjectural claims, but must be grounded in demonstrable need and credible evidence.

Ultimately, the application was dismissed with costs. The Court found that the applicant had failed to establish a prima facie right to the information, had not demonstrated irreparable harm, and that the balance of convenience favoured maintaining the confidentiality of ballot paper security features. The decision is significant for access to information jurisprudence as it illustrates the limits of transparency where competing constitutional values - such as public security and electoral integrity - are at stake. It also affirms that the right to information is conditioned on necessity and relevance, and that courts will defer to constitutionally mandated bodies in matters falling within their specialised expertise unless there is clear evidence of abuse or illegality.

Blessed Mhlanga v Magistrate Nduna NO & Others[37] HH 584/21

In **Blessed Mhlanga v Magistrate Nduna NO & Others**, the applicant, a journalist, sought to invoke sections 61 and 62 of the Constitution to compel access to the full record of proceedings in State v Hopewell Chin'ono, including portions that had been heard in camera. During the bail proceedings in that matter, the presiding magistrate had granted an application by the prosecution for certain evidence relating to prison conditions and COVID-19 protocols to be heardin camera on the basis of prison security concerns, resulting in the exclusion of the public and the media. The applicant challenged this decision and sought a mandatory interdict compelling the respondents to release the complete record, as well as declaratory relief that the in camera proceedings were unlawful and unconstitutional. He further challenged the constitutionality of section 3 of the Courts and Adjudicating Authorities (Publicity Restriction) Act.

The High Court dismissed the application and in doing so clarified several important principles relating to access to information, media rights, and procedural discipline in constitutional litigation. The Court first held that the respondents cited were not the proper custodians of the court record. In terms of section 6(2) of the Courts and Adjudicating Authorities Act, custody of court records lies with designated officers such as magistrates generally or court registrars, and not necessarily with the presiding magistrate or the Prosecutor-General. The first respondent was functus officio and no longer in possession of the record, rendering any order against the cited parties ineffective.

The Court further found that although the applicant framed his claim as a constitutional challenge, the substance of the relief sought amounted to a collateral attack on the magistrate's ruling to conduct proceedings in camera. Such a challenge could only properly be brought through appeal or review proceedings. The applicant, not being a party to the original proceedings and being out of time, could not circumvent established procedural rules by recasting the matter as a constitutional application.

A central aspect of the judgment concerned the proper invocation of section 62 of the Constitution. The Court emphasised that access to information is not self-executing and must be exercised in accordance with enabling legislation, in this case the Freedom of Information Act. The applicant had failed to demonstrate that he had made a formal request for the information through the statutory mechanism or that such a request had been refused. The Court held that where legislation provides a specific procedure for accessing information, that procedure must be exhausted before constitutional relief is sought. Furthermore, the applicant failed to specify the capacity in which he approached the court under section 85 of the Constitution, whether in his own interest, in the public interest, or in a representative capacity, which rendered his reliance on constitutional rights procedurally defective.

The Court also observed that the applicant's stated objective of informing the public about prison conditions could have been achieved through less intrusive means, such as obtaining information directly from the accused person or pursuing access through appropriate channels directed at prison authorities. It considered the insistence on accessing the specific in camera evidence as

37. Blessed Mhlanga v Magistrate Nduna N.O. & Others HH 584/21, High Court of Zimbabwe, on access to court records, in camera proceedings and exhaustion of statutory remedies.

unnecessary and unjustified in the circumstances.

With respect to the constitutional challenge to section 3 of the Courts and Adjudicating Authorities Act, the Court held that the application was fatally defective due to non-joinder of necessary parties, including Parliament and the Attorney-General. It reiterated that any challenge to the validity of legislation must involve all parties with a direct legal interest in the law, failing which the proceedings are incompetent.

Importantly, the Court reaffirmed that fundamental rights, including freedom of expression and access to information, are subject to limitation under section 86 of the Constitution. It accepted that in camera proceedings may be justified where necessary to protect legitimate interests such as prison security, and that courts retain discretion to restrict public access to proceedings in appropriate circumstances. The judgment makes it clear that journalists do not enjoy automatic or unfettered access to all court records or proceedings, particularly where competing constitutional interests arise.

The decision is significant for access to information litigation as it underscores the importance of procedural compliance, including proper standing, exhaustion of statutory remedies, and correct joinder of parties. It also clarifies that the right of access to information does not extend to overriding judicial determinations made in accordance with the law, and that constitutional litigation cannot be used as a substitute for appeal or review. The case therefore highlights the balance between transparency and other legitimate interests such as security, while reinforcing the structured and rule-bound nature of constitutional enforcement.

CHAPTER 05

Data Protection and Privacy

Data protection and the right to privacy have emerged as central pillars of constitutional governance in the digital age, particularly in light of the rapid expansion of digital technologies, surveillance capabilities, and data-driven decision-making. In Zimbabwe, the right to privacy is constitutionally guaranteed under section 57[38] of the Constitution, which protects individuals against arbitrary interference with their privacy, family, home, or correspondence, as well as unlawful collection, storage, use, or dissemination of personal information. This provision establishes a substantive and enforceable right that applies to both State and non-State actors.

The constitutional protection of privacy is closely linked to other fundamental rights, including freedom of expression under section 61, access to information under section 62, and dignity under section 51. In the digital environment, these rights frequently intersect and, at times, come into tension. For example, the collection and dissemination of personal data may facilitate access to information and public accountability, while simultaneously posing risks to individual privacy and autonomy. Courts are therefore increasingly required to strike a careful balance between transparency, public interest, and the protection of personal data.

Zimbabwe has taken legislative steps to give effect to the right to data protection through the enactment of the Cyber and Data Protection Act [Chapter 12:07]. This statute regulates the collection, processing, storage, and use of personal data, establishes principles of lawful data processing, and imposes obligations on data controllers and processors to ensure the protection of personal information. It also introduces offences relating to unlawful access, data breaches, and misuse of information, reflecting the growing recognition of data governance as a critical aspect of human rights protection.

Notwithstanding these developments, the legal framework remains in a state of evolution. Concerns persist regarding the breadth of State surveillance powers, the adequacy of safeguards against abuse, and the extent to which data protection principles are effectively implemented in practice. In addition, the increasing role of private actors, including telecommunications companies, digital platforms, and financial service providers, raises complex questions regarding accountability, consent, and cross-border data flows.

Comparative and regional jurisprudence has played an important role in shaping the understanding of data protection and privacy rights. Courts across jurisdictions have increasingly recognised informational privacy as an essential component of human dignity and personal

38. Constitution of Zimbabwe Amendment (No. 20) Act, 2013, ss 51, 57, 61, 62 and 86; Cyber and Data Protection Act [Chapter 12:07].

autonomy, particularly in the context of mass data collection, biometric systems, and digital surveillance. These developments are also reflected in international and regional instruments, including the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), which emphasises the need for robust legal frameworks to safeguard personal data.

The cases discussed in this chapter illustrate the emerging contours of data protection and privacy jurisprudence, highlighting key principles such as the requirement of lawful and justified interference with privacy, the need for proportionality in data processing and surveillance measures, and the obligation on both State and private actors to respect and protect personal information. They also demonstrate the increasing role of courts in mediating the tension between technological advancement and the preservation of fundamental rights in a digital society.

5.1 Data Privacy and Data Protection

Data privacy and data protection have become increasingly important because modern life depends on constant data collection, data sharing and digital communication. The right to privacy now extends beyond the traditional protection of the home, family and correspondence, and includes the protection of personal information, anonymity, confidential communications, journalistic sources and freedom from unlawful surveillance. Privacy is also becoming an important cause of action in litigation, including claims based on breach of privacy, breach of confidentiality, misuse of private information, malicious falsehood and data breaches.

Privacy is especially important for journalists, activists, whistleblowers and human rights defenders because it enables freedom of expression. It allows people to share unpopular or sensitive views anonymously without fear of punishment, protects whistleblowers who disclose information in the public interest, and enables journalists and activists to communicate securely without unlawful interception. Without privacy, freedom of expression may be chilled because people may fear that their communications, identities or sources will be exposed.

International law recognises privacy as a fundamental right[39]. Article 12 of the Universal Declaration of Human Rights provides that no one shall be subjected to arbitrary interference with their privacy, family, home or correspondence, or to attacks on their honour and reputation. Article 17 of the International Covenant on Civil and Political Rights contains similar protection and requires States to protect individuals against unlawful or arbitrary interference with privacy. However, privacy is not absolute. It may be limited where the interference is lawful, necessary and reasonable in a democratic society. The UN Human Rights Committee's General Comment No. 16 explains that interference with privacy must be authorised by law, and that the law itself must comply with the aims and objectives of the Covenant. It also explains that even interference provided for by law may still be arbitrary if it is unreasonable in the circumstances.

The relationship between privacy and freedom of expression requires courts to conduct a careful balancing exercise[40]. This is usually done on a case-by-case basis. Relevant factors include whether the publication concerns a matter of public interest, whether the affected person is a

39. Universal Declaration of Human Rights, art 12; International Covenant on Civil and Political Rights, art 17; UN Human Rights Committee, General Comment No. 16 on the right to privacy.
40. See generally Axel Springer AG v Germany App no 39954/08 (ECtHR, Grand Chamber, 7 February 2012); Mosley v United Kingdom App no 48009/08 (ECtHR, 10 May 2011).

public figure, how the information was obtained, whether the information is reliable, and whether the expression contributes to a debate of general public importance. These principles are reflected in cases such as **Uuter Dery [41]and Others v Ghana, Axel Springer AG v Germany and Mosley v United Kingdom**. In Uuter Dery, the ECOWAS Court accepted that the recording and filming of the applicants interfered with their privacy, but held that the interference was lawful and necessary in a democratic society because it was aimed at preventing and exposing crime.

Data protection is one of the main legal mechanisms through which the right to privacy is protected. Data protection laws regulate how personal information is collected, processed, stored, shared and transferred. Personal data generally means information relating to an identified or identifiable person, such as a name, identification number, location data, biometric data, communication records or online identifiers. Effective data protection laws require personal information to be processed fairly and lawfully, collected for a specific purpose, kept accurate and up to date, retained only for as long as necessary, protected against unauthorised access or loss, and transferred across borders only where adequate safeguards exist.

In Africa, data protection is developing through regional and domestic legal frameworks. Important regional instruments include the African Union Convention on Cyber Security and Personal Data Protection[42], also known as the Malabo Convention, and the ECOWAS Supplementary Act on Personal Data Protection. Domestic examples include Ghana's Data Protection Act, South Africa's Protection of Personal Information Act, Nigeria's data protection framework and Kenya's Data Protection Act. These laws generally reflect principles similar to those found in the European Union's General Data Protection Regulation, including accountability, lawfulness, consent, purpose limitation, data minimisation, data subject rights and security safeguards.

Data protection laws must also accommodate journalism and freedom of expression. If applied too rigidly, data protection rules can undermine investigative journalism[43], public interest reporting and civic accountability. Article 85 of the GDPR requires States to reconcile the right to data protection with freedom of expression and information, including processing for journalistic, academic, artistic or literary purposes. The Court of Justice of the European Union has adopted a functional approach to journalism, meaning that even individuals who are not formally recognised as journalists may benefit from journalistic exemptions where their purpose is to disclose information, opinions or ideas to the public.

For public interest lawyers, this area is important because privacy and data protection litigation can be used both defensively and offensively. It can protect journalists and sources against unlawful surveillance, challenge overbroad State data collection, seek remedies for data breaches, and contest laws that fail to provide adequate safeguards. At the same time, lawyers must ensure that privacy claims are not used to suppress legitimate public interest reporting, whistle-blowing or criticism of public officials. The central question is whether the restriction or interference is lawful, necessary, proportionate and justified in a democratic society.

41. Uuter Dery and Others v Ghana, ECOWAS Court of Justice, on privacy, recording/filming and public interest exposure of wrongdoing.
42. African Union Convention on Cyber Security and Personal Data Protection, adopted 27 June 2014; ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection.
43. Regulation (EU) 2016/679, General Data Protection Regulation, art 85, requiring reconciliation of data protection with freedom of expression and information.

Government digital surveillance

Government digital surveillance is one of the most serious modern threats[44] to privacy, freedom of expression, journalism and civic participation. Communications surveillance includes the monitoring, interception, collection, analysis, retention or use of information relating to a person's communications, whether in the past, present or future. It may involve access to the content of communications, such as calls, emails and messages, or to metadata, such as location data, contact patterns, device identifiers and connection records. Although metadata may appear less intrusive than content, it can reveal highly sensitive information about a person's movements, associations, sources, political activity and private life.

Unlawful or arbitrary surveillance violates the right to privacy and can also interfere with freedom of expression. Where surveillance is conducted on a mass scale, it may contradict the basic principles of a democratic society because it enables the State to monitor lawful political activity, journalism, activism and private communication. International standards require that the integrity and confidentiality of correspondence must be protected both in law and in practice. Surveillance of digital communications must therefore be based on a legal framework that is public, clear, precise, comprehensive and non-discriminatory.

Surveillance may only be justified where it satisfies strict legality, necessity and proportionality requirements. Before conducting communications surveillance, the State should be required to demonstrate before a competent and independent judicial authority that there is a high probability that a serious crime or specific threat to a legitimate aim has occurred or will occur, and that the surveillance is likely to obtain evidence relevant to that threat. The State must also show that less intrusive methods have been exhausted or would be ineffective, that the information collected will be limited to what is relevant and necessary, and that any excess information will be promptly destroyed or returned. The surveillance must be limited to a specified authority, purpose and duration, and must not undermine the essence of the right to privacy or other fundamental freedoms.

The protection of journalistic sources is a particularly important aspect of privacy in the surveillance context. Surveillance can expose confidential sources, chill investigative reporting and undermine newsroom security. If whistleblowers and sources fear that their communications with journalists may be intercepted or traced, they may avoid disclosing information of public interest. For this reason, interference with journalistic sources should only be permitted where there is an overriding requirement in the public interest, such as the investigation or prevention of a serious crime, and only where the information cannot reasonably be obtained by other means. Such interference should be authorised by a court after a full hearing and must be subject to independent safeguards.

The African Commission's Declaration of Principles on Freedom of Expression and Access to Information[45] recognises that media practitioners should not be compelled to reveal confidential sources or disclose journalistic material unless strict conditions are met.

44. UN Human Rights Council, The Right to Privacy in the Digital Age, A/HRC/RES/42/15 and related OHCHR reports on privacy in the digital age.
45. African Commission on Human and Peoples' Rights, Declaration of Principles on Freedom of Expression and Access to Information in Africa, 2019, Principles 25, 35, 37-42.

These include that the identity of the source is necessary for the investigation or prosecution of a serious crime or for the defence of an accused person, that the information cannot be obtained elsewhere, that the public interest in disclosure outweighs the harm to freedom of expression, and that disclosure has been ordered by a court. These standards are especially important in the digital age because source disclosure may occur not only through direct court orders but also indirectly through phone records, email metadata, spyware and device surveillance.

Surveillance takes several forms. Phone tapping involves interception of the content of calls or text messages. Bulk interception involves large-scale capture of communications, often for intelligence purposes. Data retention requires service providers to store traffic, location or subscriber data for possible future use by authorities. Spyware involves the covert compromise of a person's device, sometimes through zero-click exploits, allowing access to messages, files, microphones, cameras, call logs and cloud accounts. Spyware is especially dangerous because it can defeat end-to-end encryption by accessing information directly from the device before or after encryption.

Comparative jurisprudence provides important guidance on the safeguards required for lawful surveillance. In Big Brother Watch and Others v United Kingdom[46], the European Court of Human Rights held that bulk interception regimes may be compatible with the Convention only where they contain robust end-to-end safeguards. The Court found violations because the United Kingdom's regime lacked adequate independent authorisation, selector safeguards and protections for journalistic material. The case is important because it recognises that surveillance measures affecting journalists require heightened protection, especially where search terms or selectors are linked to journalists or may expose confidential sources.

In **Roman Zakharov v Russia**[47], the European Court of Human Rights found that Russia's secret interception framework violated the right to privacy because it failed to provide adequate safeguards against arbitrariness and abuse. The Court accepted that a person could challenge a surveillance system even without proving that they had personally been intercepted, because the broad scope of the system and lack of effective remedies created a systemic risk. The judgment is useful for strategic litigation because it supports standing based on systemic exposure to surveillance powers and establishes that secret interception regimes must contain clear rules on scope, duration, authorisation, supervision, notification and remedies.

In Digital Rights Ireland[48], the Court of Justice of the European Union invalidated the EU Data Retention Directive because it required generalised and indiscriminate retention of traffic and location data. The Court held that such retention constituted a serious interference with privacy and data protection rights and lacked adequate limits, independent review and security safeguards. The case is particularly important for journalists because metadata can reveal sources, networks and patterns of communication even without accessing the content of messages. In Schrems[49]II, the same Court invalidated the EU-US Privacy Shield because United States surveillance laws did not provide adequate safeguards or effective judicial remedies, highlighting the risks of cross-border data transfers where foreign intelligence agencies may access personal data.

46. Big Brother Watch and Others v United Kingdom Apps nos 58170/13, 62322/14 and 24960/15 (ECtHR, Grand Chamber, 25 May 2021), on bulk interception safeguards and journalistic material.
47. Roman Zakharov v Russia App no 47143/06 (ECtHR, Grand Chamber, 4 December 2015), on secret surveillance systems and safeguards against abuse.
48. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others Joined Cases C-293/12 and C-594/12 (CJEU, 8 April 2014), on indiscriminate data retention
49. Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems Case C-311/18 (CJEU, 16 July 2020), on cross-border transfers, surveillance safeguards and effective remedies..

African and Global South jurisprudence is also emerging. In Kenya, litigation challenging requirements for individuals to declare IMEI numbers of mobile devices has raised concerns that device identifiers, when combined with subscriber data held by mobile service providers, may enable identification and tracking of individuals and become a gateway to mass surveillance. The argument in such cases is that where a State measure compels disclosure of technical identifiers capable of linking people to devices and communications, it must have a clear legal basis and satisfy strict necessity and proportionality requirements.

The Inter-American human rights system has also developed important principles. In **Escher v Brazil**[50], involving unlawful interception and dissemination of telephone conversations of rural association leaders linked to social movements, the Inter-American Court held that telephone communications fall within the right to privacy and that States must adapt legal protections to new technologies. In **Tristán Donoso v Panama**[51], where an attorney's recorded phone call was later disclosed by a public official and criminal defamation proceedings followed, the Court found violations of freedom of expression and privacy-related obligations. These cases show that unlawful interception and disclosure of communications can chill speech, undermine professional confidentiality and violate democratic rights.

Spyware such as Pegasus presents one of the gravest modern threats to privacy and independent journalism. Pegasus infections have been reported against journalists, civil society actors and human rights defenders in several countries. Such tools can provide full access to a device, including messages, calls, files, microphones, cameras and cloud tokens. For journalists, this creates serious risks of source exposure, story pre-emption, legal jeopardy and pervasive self-censorship. The growing use of spyware has led to calls for moratoria, strict judicial authorisation, independent audits, transparency, notification and effective remedies.

The comparative safeguards emerging from international courts are clear. Surveillance laws must be accessible, precise and narrowly tailored. They must prohibit generalised or indiscriminate collection. Surveillance must be authorised in advance by an independent body, preferably a court, and should be targeted to specific persons, devices or threats. There must be heightened safeguards where journalistic material or confidential sources may be affected. Data retention, security, access, deletion and sharing rules must be strictly regulated. Oversight bodies must have real powers, and affected persons should be notified once notification no longer undermines the investigation. Effective remedies must be available, including damages, exclusion of unlawfully obtained evidence and destruction of unlawfully collected data.

For rights-respecting surveillance reform, the starting point should be that targeted surveillance is the rule and mass surveillance is exceptional, if permitted at all. Any surveillance likely to capture journalist-source communications should require prior judicial authorisation and a heightened public interest test. States should publish transparency reports, maintain audit trails, empower independent oversight bodies, and ensure prompt notification where safe. Newsrooms and civil society organisations should also adopt practical risk mitigation measures, including threat modelling, secure communications, device hygiene, multi-factor authentication, hardware keys, minimisation of sensitive data storage, and incident response plans.

50. Escher and Others v Brazil, Inter-American Court of Human Rights, Judgment of 6 July 2009, on unlawful interception of telephone communications.
51. Tristán Donoso v Panama, Inter-American Court of Human Rights, Judgment of 27 January 2009, on privacy, professional confidentiality and disclosure of communications.

For public interest litigation, the strongest surveillance cases are those that combine legal argument with evidence of systemic risk, chilling effects and technological capability. Litigants should use expert forensic evidence where spyware or interception is alleged, document how surveillance affects sources and reporting, and link constitutional claims to broader legislative reform. The central argument should be that surveillance without clear law, independent authorisation, necessity, proportionality, source protection, oversight and remedies violates privacy, freedom of expression and democratic accountability.

CHAPTER 06

Right to Erasure / Right to Be Forgotten

The right to be forgotten, also known as the right to erasure, is the right of individuals to request that commercial search engines or online platforms that collect and process personal data, such as Google, remove links to personal information from search results where appropriate. This right is rooted in the broader concept of the right to private life, recognising that individuals should not be indefinitely burdened by past information about themselves where there is no continuing public interest in its accessibility.

The right does not necessarily require the deletion of the original content from the internet. Rather, it limits the prominence and accessibility of that information by preventing it from appearing in search results linked to a person's name. In this way, the information may still exist on the original website, but it is no longer easily discoverable, thereby protecting the individual's privacy and dignity while preserving the integrity of the historical record.

The principle underpinning this right is reflected in data protection frameworks such as the Data Protection Directive (DPD), which provides that personal data must be adequate, relevant, and not excessive in relation to the purpose for which it is processed. This means that where personal data becomes outdated, irrelevant, or disproportionate to its original purpose, continued indexing and dissemination may be unjustified.

Importantly, the right to be forgotten is not absolute. It requires a careful balancing between the individual's rights to privacy and data protection and the public's right to access information, as well as freedom of expression. Factors such as whether the individual is a public figure, the nature of the information, its accuracy, the time elapsed, and the continuing public interest all play a critical role in determining whether delisting is justified.

The decision in **Google Spain v González (2014)**[52] is the leading authority establishing the modern right to be forgotten in digital law. The Court of Justice of the European Union held that search engines such as Google are data controllers and can be required to remove or conceal links to personal information appearing in search results. The case arose from a complaint by an individual who objected to links to newspaper reports about past legal proceedings being easily accessible through a search of his name.

The Court ruled that individuals have the right to request delisting where the search results are inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which the data was originally processed. Importantly, the Court emphasised that this right is not automatic. A fair balance must always be struck between the individual's fundamental rights to privacy and

52. Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González Case C-131/12 (CJEU, 13 May 2014), on search engines and the right to de-indexing.

data protection and the public's interest in accessing the information. In conducting this balancing exercise, courts must consider factors such as the nature of the information, its sensitivity for the individual's private life, and the level of public interest in continued access, particularly where the individual plays a role in public life.

Subsequent developments have refined and tested the scope of this right. In Biancardi v Italy, the European Court of Human Rights considered whether obligations relating to de-indexing could extend beyond search engines to other actors, including journalists or website operators. The Court defined de-indexing as the removal of links from search results that connect a person's name to third-party content. However, the case introduced a more nuanced approach where the person responsible for the content was not a search engine but a publisher.

Applying a proportionality analysis, the Court examined factors such as the length of time the material remained online after the request for removal, the sensitivity of the data, and the severity of any sanction imposed on the publisher. It ultimately found no violation of freedom of expression, recognising that journalistic archives and public records serve an important role in preserving information of public interest.

Together, these cases demonstrate that the right to be forgotten is evolving and context-dependent. While Google Spain established the obligation on search engines to limit access to certain personal data, later cases such as Biancardi show that courts are cautious about extending this obligation to journalists or content creators, particularly where doing so may interfere with media freedom and the public's right to know.

In Hurbain v Belgium, the Grand Chamber of the European Court of Human Rights addressed a more advanced dimension of the right to be forgotten - whether individuals can require the anonymisation of information contained in online news archives. Unlike earlier cases that focused primarily on de-indexing by search engines, this case concerned the continued publication of lawfully archived journalistic content and whether altering that content (through anonymisation) was justified.

The Court accepted that, in certain circumstances, anonymisation of archived material may be an appropriate remedy to balance privacy rights with freedom of expression. However, it emphasised that such a remedy requires a careful and context-specific proportionality assessment. The Grand Chamber set out a refined set of criteria to guide this balancing exercise. These include the nature of the archived information, the time that has elapsed since the events and the original publication, the current public interest in the information, whether the individual is a public figure and how they have conducted themselves since the events, the negative consequences of continued online availability, the level of accessibility of the information in digital archives, and the potential impact of anonymisation on freedom of expression, particularly press freedom.

These criteria represent a development from earlier jurisprudence because they respond specifically to the unique challenges posed by digital archives, where information remains

permanently accessible and searchable long after its original publication. The Court recognised that while archives serve an essential role in preserving history and supporting media freedom, the indefinite accessibility of personal information can, in some cases, cause disproportionate harm to individuals.

Comparative approaches show that courts have generally been cautious in extending the right to be forgotten beyond search engines. In jurisdictions such as Argentina and India, courts have been more willing to order de-indexing against search engines or social media platforms but have typically resisted requiring news organisations to alter or remove content from their archives. This reflects a strong concern for protecting the integrity of the historical record and the role of the media.

Similarly, the Supreme Court of Japan has taken a restrictive approach, emphasising that decisions to remove information from search results should prioritise the public's right to access information. In India, the Madras High Court rejected a request to anonymise court records in a case involving an acquitted individual, holding that the right to be forgotten cannot override the need to preserve information that serves a public interest function, such as maintaining judicial records.

Taken together, these developments show that while the right to be forgotten is increasingly recognised, its application becomes more limited as it moves closer to core areas of public interest, such as journalism, court records and historical archives. Courts are more willing to intervene where search engines amplify access to personal data, but they are far more cautious where remedies would alter original publications or undermine the integrity of public records.

Encryption and Anonymity on the Internet

Encryption and anonymity are essential tools for the effective enjoyment of digital rights, particularly the rights to privacy and freedom of expression. They enable individuals to communicate securely, share ideas without fear of retaliation, and resist censorship in both democratic and restrictive environments. In practical terms, encryption refers to the process of converting messages or data into a form that is unreadable to anyone except the intended recipient, thereby safeguarding the confidentiality and integrity of communications against unauthorised access or interference. Anonymity, on the other hand, allows individuals to communicate or act without revealing their identity, either by remaining completely unidentified or by using pseudonyms, which can be selectively disclosed where necessary.

These tools are particularly important for journalists, activists, whistleblowers and ordinary citizens who may face risks when expressing dissenting views or exposing wrongdoing. Anonymity allows individuals to share opinions without fear of social, political or legal consequences, while encryption ensures that their communications remain secure from interception or surveillance. In this way, both concepts are closely linked to the protection of democratic participation and open public discourse.

However, the use of encryption and anonymity is not absolute and may be subject to restrictions. Any limitation must comply with the established three-part test for restrictions on freedom of expression, namely legality, legitimacy and necessity and proportionality. This means that restrictions must be clearly provided for by law, pursue a legitimate aim such as national security or the prevention of crime, and must be necessary and proportionate in a democratic society. Blanket prohibitions on encryption or anonymity, whether in law or in practice, are generally regarded as disproportionate because they undermine the core of freedom of expression and privacy.

Targeted measures, such as decryption orders, may be permissible but only under strict conditions. They must be grounded in clear and publicly accessible legal frameworks, applied on a case-by-case basis rather than broadly, and authorised by an independent judicial authority with full respect for due process rights. International standards, including those articulated by the UN Special Rapporteur on freedom of expression, emphasise that such measures must be exceptional and justified by compelling evidence.

The importance of anonymity has been strongly recognised in comparative jurisprudence. In **McIntyre v Ohio Elections Commission**[53], the United States Supreme Court struck down a law prohibiting anonymous political campaigning, holding that anonymity is a vital safeguard for freedom of expression. The Court reasoned that anonymity protects individuals from retaliation and allows unpopular or minority views to be expressed without fear, describing it as a "shield from the tyranny of the majority." It further recognised that the decision to remain anonymous is itself an aspect of freedom of speech.

Subsequent jurisprudence in the United States has extended this protection to online environments, recognising the internet as a unique and important forum for robust and diverse debate. Courts have emphasised that the right to speak anonymously online must be carefully protected, given its role in facilitating open discourse and democratic engagement.

In addition, courts have recognised that any attempt to lift anonymity must be subject to strict safeguards. This includes prior judicial oversight, a clear legal basis, and a balancing exercise between the need to identify the individual and the broader impact on freedom of expression. In Davidoff v Google LLC, the High Court of England and Wales acknowledged the longstanding importance of anonymous speech, particularly for public commentators, noting that anonymity can be an important dimension of exercising freedom of expression.

Overall, the legal framework governing encryption and anonymity reflects a careful balancing act. While States may seek to regulate these tools in pursuit of legitimate objectives, any interference must be narrowly tailored and strictly justified. Overbroad or poorly justified restrictions risk undermining not only individual rights but also the broader democratic values that depend on secure and open communication.

In **NT1 & NT2 v Google LLC [2018] EWHC 799 (QB)**[54]**,** the High Court of England and Wales considered the scope and application of the right to be forgotten in the context of spent criminal convictions

53. McIntyre v Ohio Elections Commission 514 US 334 (1995), on anonymous political speech and freedom of expression.
54. NT1 & NT2 v Google LLC [2018] EWHC 799 (QB), on spent convictions, delisting, accuracy and continuing public interest.

and online search results. The case involved two businessmen, NT1 and NT2, who sought to compel Google to delist links to third-party reports of their past convictions, relying on data protection law and the tort of misuse of private information.

The central issues before the Court were whether the claimants were entitled to delisting on the basis that the information was inaccurate or that its continued availability unjustifiably interfered with their privacy and data protection rights, whether compensation was payable for the period during which the links remained accessible after the requests were made, and whether Google could rely on the journalistic exemption under data protection law. The Court applied the principles established in Google Spain v González and relevant EU guidance, and it rejected Google's reliance on the journalistic exemption on the basis that Google was not acting as a publisher but as a data controller and had not independently assessed the public interest prior to the complaint.

With respect to NT1, the Court rejected both the inaccuracy claim and the right to be forgotten claim. It found that the information contained in the links was not misleading when assessed from the perspective of an ordinary reader. More importantly, the Court held that NT1 did not have a reasonable expectation of privacy. He was considered a public figure in the business sphere, and the information related to serious business crime, prosecution and punishment, which remained matters of legitimate public interest. The Court emphasised that the information originated from lawful court reporting and that its publication was a foreseeable consequence of his own conduct. It also took into account his post-conviction behaviour, including his failure to show remorse and his misleading conduct, which reinforced the continuing relevance of the information. As a result, his claim for delisting and damages was dismissed.

In contrast, NT2 succeeded in part. The Court found that one of the articles was inaccurate in that it misrepresented the nature and extent of his criminal conduct, suggesting financial gain where none had been established. More significantly, the Court held that the continued availability of the links was no longer justified. The information had become outdated and irrelevant, and there was no sufficient legitimate interest in maintaining its accessibility through search results. The Court considered several factors, including that the conviction had become spent, that NT2's current business activities were unrelated to his past conduct, that the offence did not involve dishonesty in a way that would affect his present reputation, and that he had pleaded guilty and demonstrated remorse. These factors supported the conclusion that his privacy and data protection rights outweighed the public interest in continued access to the information.

However, despite succeeding on the delisting claim, NT2 was not awarded compensation. The Court accepted that Google had taken reasonable steps to comply with its data protection obligations and therefore could rely on the statutory defence under the Data Protection Act. The Court ultimately ordered that the relevant links relating to NT2 be removed, while NT1's claim was dismissed in its entirety. Permission to appeal was granted to NT1, with the Court noting that such claims were likely to increase following the recognition of the right to be forgotten.

The case is significant because it demonstrates the nuanced and fact-specific nature of the right to be forgotten. It confirms that a spent conviction does not automatically entitle a person to delisting. Courts will undertake a detailed balancing exercise, considering the individual's role in public life, the nature of the offence, the time elapsed, the accuracy of the information, and the individual's conduct since the events. It also reinforces that search engines are data controllers with independent obligations and that the right to be forgotten is a limited remedy aimed at reducing unjustified harm from continued digital exposure rather than erasing historical facts.

The right of erasure, commonly known as the "right to be forgotten," is the right of individuals to request that search engines remove links to personal information about them where that information is inadequate, irrelevant, no longer relevant, or excessive in relation to the purpose for which it was originally processed. This right does not operate in absolute terms; rather, it requires a careful balancing between the individual's rights to privacy and data protection and the public's right to access information, as well as freedom of expression.

The legal foundation for this right is grounded in the decision of the Court of Justice of the European Union in Google Spain v González, which established that search engines such as Google are "controllers" of personal data and must ensure that their processing complies with data protection law. When a delisting request is made, the search engine - and ultimately the court - must conduct a balancing exercise between the individual's fundamental rights to privacy and data protection and the legitimate interest of the public in accessing the information.

In undertaking this balancing exercise, several factors are relevant. These include the nature of the information, particularly whether it relates to private life or public or business activities; the sensitivity of the information and its impact on the individual's privacy; the level of public interest in accessing the information; the original context and source of the publication; and whether the information is inaccurate, outdated, or no longer relevant. These considerations ensure that the right to be forgotten operates in a principled and context-sensitive manner rather than as an automatic entitlement.

The jurisprudence further establishes a number of important principles. Individuals who play a role in public life, especially in business or commercial contexts, have a reduced expectation of privacy, particularly in relation to information concerning business misconduct or criminal activity. Information will continue to be regarded as relevant where it bears on the individual's current activities and the public's assessment of their honesty and integrity. The nature of the offence is also important, with crimes involving dishonesty more likely to retain public interest relevance than those that do not. Post-conviction conduct is equally significant: acceptance of responsibility, remorse and evidence of rehabilitation may support delisting, whereas denial, misleading behaviour and lack of remorse may weigh against it.

The fact that a conviction has become "spent" does not automatically entitle an individual to have links removed. The question remains whether there is a continuing public interest in access to the information. Similarly, while inaccuracy or misleading information strengthens a claim for delisting, it does not automatically compel removal and must be considered alongside other

factors. Even where delisting is granted, compensation is not automatic; it may be refused where the search engine has taken reasonable steps to comply with its legal obligations.

Ultimately, the courts have emphasised that the right to be forgotten is not a mechanism for rewriting history or erasing past events. The original source material will ordinarily remain accessible.The remedy is limited to reducing the prominence of the information in search results. The right must therefore always be balanced against freedom of expression and the public's right to know, particularly where the individual remains active in public life or where the information continues to serve a legitimate public interest.

Website/Platform Blocking Cases

In **Ahmet Yildirim v Turkey**[55], the European Court of Human Rights dealt with the legality of broad website and platform blocking measures and their impact on freedom of expression. The applicant, who operated a lawful academic website hosted on Google Sites, was affected when a Turkish court ordered the blocking of an entirely different website on the same platform. In implementing that order, the authorities blocked access to the whole Google Sites domain, thereby rendering the applicant's lawful website inaccessible.

The Court identified three central issues: whether the blocking measure constituted an interference with the applicant's right to freedom of expression under Article 10, whether the interference was "prescribed by law" with adequate safeguards against arbitrariness, and whether the domestic legal framework provided sufficient protection against disproportionate and collateral effects.

The Court held that the measure clearly constituted interference with freedom of expression, as it prevented the applicant from receiving and imparting information through his website. Importantly, the Court emphasised that Article 10 protects not only the content of expression but also the means of its dissemination, and that the internet plays a critical role in enabling access to information in modern democratic societies. Although the blocking order was aimed at unlawful content on a different website, its collateral effect was to suppress lawful expression, which heightened the seriousness of the interference.

In assessing whether the interference was justified, the Court examined whether it met the requirements of Article 10(2), namely that it must be prescribed by law, pursue a legitimate aim, and be necessary in a democratic society. The Court focused in particular on the "quality of law" requirement, which demands that legislation be accessible, clear, and foreseeable in its application. It found that the Turkish legal framework, specifically Law No. 5651, was deficient because it did not clearly authorise wholesale platform blocking and contained vague and conflicting provisions. The law failed to define the scope of blocking powers adequately and did not provide safeguards to prevent overbroad application.

The Court further criticised the domestic authorities for failing to consider less restrictive alternatives. The national court had accepted the administrative authority's claim that blocking

53. McIntyre v Ohio Elections Commission 514 US 334 (1995), on anonymous political speech and freedom of expression.
54. NT1 & NT2 v Google LLC [2018] EWHC 799 (QB), on spent convictions, delisting, accuracy and continuing public interest.
55. Ahmet Yildirim v Turkey App no 3111/10 (ECtHR, 18 December 2012), on overbroad website blocking and Article 10 ECHR.

the entire platform was the only technical solution, without investigating whether more targeted measures, such as blocking a specific URL, could have achieved the same objective. There was no meaningful balancing of competing interests, nor any assessment of proportionality. Additionally, the legal framework allowed administrative bodies to expand blocking orders without proper judicial scrutiny, and it lacked effective mechanisms for affected parties to challenge such measures.

As a result, the Court concluded that the interference was neither foreseeable nor accompanied by adequate safeguards, and that it produced arbitrary and disproportionate effects. By blocking all websites hosted on the platform, the measure went far beyond what was necessary to address the offending content. The Court therefore found a violation of Article 10.

The case establishes important principles for digital rights. It confirms that wholesale platform blocking is inherently suspect under freedom of expression standards, particularly where it affects lawful content. It underscores the need for precise and narrowly tailored measures, robust legal safeguards, and meaningful judicial oversight. Most importantly, it affirms that states must avoid overbroad restrictions that sacrifice access to lawful information in the pursuit of controlling unlawful content, reinforcing the principle that rights to freedom of expression apply "regardless of frontiers."

Building on Ahmet Yildirim v Turkey, the Court's reasoning - particularly as reinforced by the separate opinion of Judge Pinto de Albuquerque - sets out a detailed framework for what lawful and rights-compliant internet blocking should look like.

The concurring opinion outlines minimum safeguards that any legal regime authorising website or platform blocking must include. These safeguards require clear definitions of who may be targeted, what types of blocking orders are permissible (such as specific URLs, IP addresses or domains), the territorial scope and duration of such orders, and the legitimate aims that may justify interference. Crucially, the framework insists on proportionality and necessity, meaning that any restriction must go no further than required to achieve its purpose. It also requires that only properly authorised bodies issue reasoned decisions, that affected parties are notified and, where possible, heard, and that there is access to effective judicial review.

A central principle emerging from the case is that indiscriminate or overbroad blocking measures are inherently unlawful. Where a measure intended to target specific illegal content results in the suppression of lawful content - simply because it shares the same platform - it fails the requirement of adequacy and proportionality. In such circumstances, there is no rational connection between the interference and the objective pursued. The Court made it clear that indefinite or wide-ranging blocking orders amount to a form of prior restraint and, in effect, censorship.

The case therefore establishes several key principles. First, blocking entire platforms or domains to address isolated unlawful content constitutes an unjustified interference with freedom of expression. Second, access to the internet itself is protected under freedom of expression, as it is

now a primary means of communication and information dissemination. Third, laws authorising blocking must meet strict "quality of law" standards, meaning they must be clear, precise and foreseeable in their application. Fourth, courts must always assess whether less restrictive alternatives - such as targeting a specific page or piece of content - can achieve the same aim. Administrative convenience, such as claiming that a broad block is the "only practical option," is not a sufficient justification.

The judgment also emphasises the importance of procedural safeguards. Any blocking regime must ensure that affected parties are given notice, that there is a proper balancing of competing interests, and that courts undertake a genuine assessment of necessity and proportionality. It must also account for third-party impacts, recognising that innocent users and content providers may be affected by broad measures. Where administrative bodies are involved, their powers must be tightly controlled and subject to meaningful judicial oversight to prevent abuse.

The broader implication of the case is that website and platform blocking is not an ordinary regulatory tool but a severe restriction on fundamental rights. It must therefore be treated as exceptional and subject to the highest level of scrutiny. The Court's message is clear: States must adopt narrowly tailored, targeted measures rather than broad, sweeping restrictions. In simple terms, they must use "surgical" interventions rather than "carpet bombing" the digital space.

Why Zimbabwe Public Interest litigation lawyers should be concerned with platform blocking

Zimbabwe should be concerned about website or platform blocking because it constitutes a form of prior restraint that directly undermines constitutional rights to freedom of expression and access to information under sections 61 and 62 of the Constitution. International jurisprudence, particularly Ahmet Yildirim v Turkey, makes it clear that blocking entire platforms in order to target specific unlawful content results in collateral censorship, where lawful information is suppressed alongside the targeted material, rendering such measures disproportionate and inconsistent with democratic standards.

This concern is not merely theoretical. Zimbabwe has already experienced unlawful restrictions on digital access, most notably in Zimbabwe Lawyers for Human Rights v Minister of State for National Security, where the High Court set aside a nationwide internet shutdown for lack of legal authority. Although the decision affirmed judicial oversight, it also exposed the vulnerability of digital rights to executive overreach. At the same time, recent legislative developments, including the Cyber and Data Protection Act, the Broadcasting Services Amendment Act, and the so-called Patriotic Act, signal an expansion of state power over digital spaces, raising the risk that platform blocking could be normalised as a regulatory tool.

Platform blocking also produces far-reaching economic and social consequences. In a digital economy, access to online platforms is essential for education, healthcare delivery, commerce, and civic participation. Blocking platforms disrupts these services, disproportionately affecting ordinary citizens, small businesses, and vulnerable groups. It also undermines the principle that rights apply "regardless of frontiers," a core element of international human rights law governing

digital communication.

Importantly, Zimbabwean courts have demonstrated a willingness to safeguard digital rights, as seen in Zimbabwe Online Content Creators Trust v Zimbabwe Media Commission, where the High Court resisted administrative overreach in regulating online media. However, wholesale platformblocking would likely fail constitutional scrutiny because it cannot meet the strict test that limitations on rights must be fair, reasonable, necessary, and justifiable in a democratic society. Where less restrictive measures - such as targeted removal of specific unlawful content - are available, broad blocking measures are inherently disproportionate.

In essence, the risk for Zimbabwe is that platform blocking shifts the regulatory approach from precise, accountable intervention to blunt, sweeping censorship, undermining both constitutional guarantees and the country's broader democratic and economic development trajectory.
Encryption and Anonymity on the Internet

Encryption and anonymity are essential tools for the effective enjoyment of digital rights, particularly the rights to privacy and freedom of expression. They enable individuals to communicate securely, share ideas without fear of retaliation, and resist censorship in both democratic and restrictive environments. In practical terms, encryption refers to the process of converting messages or data into a form that is unreadable to anyone except the intended recipient, thereby safeguarding the confidentiality and integrity of communications against unauthorised access or interference. Anonymity, on the other hand, allows individuals to communicate or act without revealing their identity, either by remaining completely unidentified or by using pseudonyms, which can be selectively disclosed where necessary.

These tools are particularly important for journalists, activists, whistleblowers and ordinary citizens who may face risks when expressing dissenting views or exposing wrongdoing. Anonymity allows individuals to share opinions without fear of social, political or legal consequences, while encryption ensures that their communications remain secure from interception or surveillance. In this way, both concepts are closely linked to the protection of democratic participation and open public discourse.

However, the use of encryption and anonymity is not absolute and may be subject to restrictions. Any limitation must comply with the established three-part test for restrictions on freedom of expression, namely legality, legitimacy and necessity and proportionality. This means that restrictions must be clearly provided for by law, pursue a legitimate aim such as national security or the prevention of crime, and must be necessary and proportionate in a democratic society. Blanket prohibitions on encryption or anonymity, whether in law or in practice, are generally regarded as disproportionate because they undermine the core of freedom of expression and privacy.

Targeted measures, such as decryption orders, may be permissible but only under strict conditions. They must be grounded in clear and publicly accessible legal frameworks, applied on a case-by-case basis rather than broadly, and authorised by an independent judicial authority

with full respect for due process rights. International standards, including those articulated by the UN Special Rapporteur on freedom of expression, emphasise that such measures must be exceptional and justified by compelling evidence.

The importance of anonymity has been strongly recognised in comparative jurisprudence. In McIntyre v Ohio Elections Commission, the United States Supreme Court struck down a law prohibiting anonymous political campaigning, holding that anonymity is a vital safeguard for freedom of expression. The Court reasoned that anonymity protects individuals from retaliation and allows unpopular or minority views to be expressed without fear, describing it as a "shield from the tyranny of the majority." It further recognised that the decision to remain anonymous is itself an aspect of freedom of speech.

Subsequent jurisprudence in the United States has extended this protection to online environments, recognising the internet as a unique and important forum for robust and diverse debate. Courts have emphasised that the right to speak anonymously online must be carefully protected, given its role in facilitating open discourse and democratic engagement.

In addition, courts have recognised that any attempt to lift anonymity must be subject to strict safeguards. This includes prior judicial oversight, a clear legal basis, and a balancing exercise between the need to identify the individual and the broader impact on freedom of expression. In Davidoff v Google LLC, the High Court of England and Wales acknowledged the longstanding importance of anonymous speech, particularly for public commentators, noting that anonymity can be an important dimension of exercising freedom of expression.

Overall, the legal framework governing encryption and anonymity reflects a careful balancing act. While States may seek to regulate these tools in pursuit of legitimate objectives, any interference must be narrowly tailored and strictly justified. Overbroad or poorly justified restrictions risk undermining not only individual rights but also the broader democratic values that depend on secure and open communication.

CHAPTER 07

Strategic Litigation Against Public Participation (SLAPPs)

This chapter examines the growing use of Strategic Litigation Against Public Participation (SLAPPs) as a tool to suppress freedom of expression, civic engagement, and accountability, particularly within the digital and public interest space. SLAPPs are not ordinary legal disputes; rather, they are carefully constructed lawsuits designed to remove information of public interest from the public domain, thereby transforming what should be matters of public debate into issues of private adjudication. This concern has been recognised in international human rights jurisprudence, including in **Velásquez Rodríguez v Honduras**, where the broader implications of silencing public discourse were highlighted.

Typically, SLAPPs are initiated under defamation law, but their scope has expanded significantly. Increasingly, claimants rely on a range of legal mechanisms - including data protection claims, allegations of breach of privacy or confidentiality, and misuse of private information - to achieve similar silencing effects. This diversification reflects an evolving legal strategy aimed at exploiting different areas of law to intimidate journalists, activists, civil society organisations, and whistleblowers who expose wrongdoing or engage in public interest advocacy.

Courts have begun to recognise the abusive nature of such litigation. A leading example is the decision of the Constitutional Court of South Africa in **Mineral Sands Resources (Pty) Ltd v Reddell**[56], where the Court acknowledged that SLAPP suits are often brought not to vindicate legitimate rights, but to silence critics and deter participation in public discourse. The Court observed that these lawsuits are typically intended to discourage political expression, limit protest, and burden opponents with costly and time-consuming legal processes, ultimately undermining democratic participation.

Against this backdrop, the chapter situates SLAPPs within the broader framework of digital rights, freedom of expression, and access to information. It highlights how such litigation strategies pose a serious threat to open societies by creating a chilling effect, where individuals refrain from speaking out due to fear of legal retaliation. The chapter further explores emerging legal responses and the role of courts in distinguishing between legitimate claims and abusive litigation designed to stifle public interest speech.

Countering SLAPPs

Effectively addressing Strategic Litigation Against Public Participation (SLAPPs) requires a clear understanding of their dual nature: first, that they arise from public participation on matters of public interest, and second, that they are characterised by abusive litigation conduct that signals

56. Reddell and Others v Mineral Sands Resources (Pty) Ltd and Others; Mineral Commodities Ltd and Another v Dlamini and Another (CCT 67/22) [2022] ZACC 38, on abusive defamation claims, public participation and SLAPPs.

a misuse of the judicial process. Identifying both elements is essential in distinguishing legitimate claims from those intended to silence, intimidate, or financially exhaust critics.

At the international level, there is growing recognition of the threat posed by SLAPPs to media freedom and democratic participation. The United Nations Human Rights Council[57], in its October 2022 resolution on the safety of journalists, expressly raised concern about the increasing use of SLAPPs to undermine the media and the public's right to information. It called on States to adopt laws and policies to prevent such litigation, provide remedies for victims, and ensure protection for journalists and media workers.

In response to this growing challenge, more structured legal frameworks are emerging. The European Union adopted an Anti-SLAPP Directive[58], which came into force in April 2024, introducing key safeguards such as early dismissal mechanisms, cost recovery provisions, and compensation for damages suffered by defendants. Significantly, the Directive has extraterritorial implications, meaning that non-EU claimants who bring cases against EU-based defendants may still be subject to these protections. Complementing this, the Council of Europe adopted a Recommendation on SLAPPs in April 2024, providing a comprehensive framework to identify and respond to abusive litigation.

The Recommendation sets out a range of indicators[59] that may signal a SLAPP, including the exploitation of power imbalances (such as political or economic influence), claims that are wholly or partially unfounded, and remedies that are disproportionate or excessive. Other indicators include attempts to increase litigation costs through delay tactics or forum shopping, targeting individuals rather than institutions, engaging in public intimidation campaigns, filing multiple or coordinated lawsuits, and refusing to engage in alternative dispute resolution mechanisms. While not all indicators must be present, the accumulation or intensity of these factors increases the likelihood that a case constitutes a SLAPP.

Crucially, the Recommendation emphasises the need for procedural safeguards. Courts and competent authorities should be empowered to assess these indicators and dismiss SLAPPs at an early stage, either wholly or partially. It further highlights the importance of mechanisms to stay proceedings while an application for dismissal is being considered, preventing claimants from escalating costs or amending pleadings to avoid dismissal. Cost-shifting measures and compensation for both pecuniary and non-pecuniary harm - such as legal expenses, loss of income, and emotional distress - are also central to deterring abusive litigation.

Beyond Europe, similar principles are gaining traction in the Americas. The Inter-American Commission on Human Rights[60], through its Special Rapporteur on Freedom of Expression, has underscored the need for States to adopt anti-SLAPP measures, including procedural tools for the prompt dismissal of such cases. These developments reflect an emerging global consensus that SLAPPs pose a systemic threat to freedom of expression, requiring proactive legal and institutional responses.

57. UN Human Rights Council, Resolution A/HRC/RES/51/9, Safety of Journalists, 12 October 2022.
58. Directive (EU) 2024/1069 of the European Parliament and of the Council of 11 April 2024 on protecting persons who engage in public participation from manifestly unfounded claims or abusive court proceedings.
59. Council of Europe Committee of Ministers, Recommendation CM/Rec(2024)2 on countering the use of strategic lawsuits against public participation (SLAPPs), adopted 5 April 2024.
60. Inter-American Commission on Human Rights, Office of the Special Rapporteur for Freedom of Expression, standards on violence, intimidation and abusive litigation against journalists and public watchdogs.

Taken together, these frameworks illustrate a shift from reactive adjudication to preventative protection, in which the law is not only used to resolve disputes but also to safeguard democratic participation by shielding individuals and organisations from litigation designed to silence them.

International and comparative developments further reinforce the need for robust responses to SLAPPs. The Inter-American Commission on Human Rights, through its Office of the Special Rapporteur for Freedom of Expression, has emphasised in its updated Inter-American Legal Framework on the Right to Freedom of Expression that States may need to adopt explicit anti-SLAPP measures, including procedural mechanisms that allow for the prompt dismissal of abusive lawsuits. This position is echoed in regional jurisprudence. In Palacio Urrutia and Others v Ecuador, the Court warned that the recurring use of judicial processes by public officials - particularly defamation or insult claims - not to seek redress but to silence criticism constitutes a serious threat to freedom of expression. Similarly, in Baraona Bray v Chile, the Court characterised such litigation as an abusive use of judicial mechanisms that States are obliged to regulate and control in order to safeguard the effective exercise of free expression.

In terms of legislative responses, anti-SLAPP frameworks have been most developed in common law jurisdictions, where statutes typically define the scope of protected expression and provide procedural safeguards for defendants. These laws vary in breadth, with some offering narrow protections and others adopting expansive definitions of public interest speech. A prominent example is the approach in California, where anti-SLAPP legislation defines protected speech broadly to include any act in furtherance of the right to petition or free expression in connection with a public issue. Under this framework, defendants must demonstrate that the claim arises from such protected activity, after which the burden shifts to the claimant to establish a probability of success.

Courts applying this framework assess whether the speech relates to a matter of public interest by considering factors such as whether the subject of the statement is a public figure, whether the conduct in question affects a broader segment of the public beyond the immediate parties, and whether the statement contributes to an ongoing debate on issues of public concern. Importantly, California law also introduces a powerful deterrent mechanism known as a “SLAPPback” action, which allows a successful defendant to institute proceedings against the claimant to recover damages arising from the abusive litigation. This remedy recognises that the harm caused by SLAPPs extends beyond legal costs to include reputational damage, emotional distress, and the broader chilling effect on public participation.

Taken together, these developments underscore an emerging global standard: that SLAPPs are not merely private disputes but systemic threats to democratic discourse, requiring both judicial vigilance and legislative intervention to ensure that courts are not weaponised to suppress public interest expression.

Good Practices for Countering SLAPPs

Effective responses to Strategic Litigation Against Public Participation (SLAPPs) require a combination of procedural safeguards, substantive legal standards, and institutional capacity. A key starting point is the development of clear indicators to assist courts and national authorities in identifying SLAPPs. These indicators - building on guidance from the Council of Europe - should include not only factors such as unfounded claims and disproportionate remedies, but also patterns like targeting individuals rather than institutions, initiating multiple or coordinated lawsuits, relying on criminal law provisions, or claiming excessive damages. Courts should also be alert to imbalances in resources between parties, as inequality of arms often signals potential abuse of process and raises broader concerns about access to justice and fair trial rights.

Importantly, respondents should not be required to prove the subjective intent of the claimant in bringing a SLAPP. Imposing such a burden would be unrealistic and would undermine the effectiveness of anti-SLAPP protections. Instead, courts should rely on objective indicators of abusive litigation conduct.

A central safeguard is the introduction of mechanisms for early dismissal of SLAPP claims. Expedited procedures allow courts to dispose of unmeritorious cases at an early stage, thereby preventing defendants from being subjected to prolonged, costly, and psychologically burdensome litigation. This is critical even in jurisdictions with strong public interest defences, as the mere existence of a defence does not prevent the chilling effect caused by the time and expense of litigation.

Closely linked to early dismissal is the need for a stay of proceedings while an anti-SLAPP application is pending. This ensures that claimants cannot continue to escalate costs through procedural tactics - such as extensive discovery or interlocutory applications - while the court is determining whether the claim itself is abusive. During this period, claimants should also be prohibited from amending their pleadings to avoid dismissal, thereby preserving the integrity of the anti-SLAPP process.

States should also ensure that defamation laws, particularly criminal defamation provisions, are not used as tools of suppression. In line with international standards, including those emphasised by the United Nations Human Rights Council, prison sentences for defamation should be abolished, and civil remedies should be preferred, provided they are proportionate and do not have a chilling effect on expression.

Financial safeguards are equally important. Introducing caps on legal costs and damages can prevent claimants from using the threat of excessive financial liability to intimidate defendants. At the same time, legal frameworks should provide for the restitution of costs and, where appropriate, compensation for damages where a SLAPP claim is dismissed. This includes both pecuniary losses - such as legal expenses and lost income - and non-pecuniary harm, including emotional distress. In particularly egregious cases, courts should consider awarding aggravated damages to deter abusive litigation.

Beyond court procedures, States have a positive obligation to strengthen institutional capacity. This includes providing targeted training for judges, lawyers, and public officials on identifying and handling SLAPPs, as well as ensuring that professional regulatory bodies enforce ethical standards to prevent lawyers from engaging in abusive litigation practices. Additionally, states should promote access to non-judicial remedies, such as mediation and alternative dispute resolution mechanisms, which can offer less adversarial and more efficient means of resolving disputes.

Finally, these measures should be understood as part of a broader obligation to protect freedom of expression and democratic participation. As reflected in jurisprudence such as Mineral Sands Resources (Pty) Ltd v Reddell, courts play a critical role in ensuring that legal processes are not weaponised to silence public interest speech. By adopting these good practices, states can move towards a legal environment where the right to participate in public debate is meaningfully protected from strategic abuse.

BIBLIOGRAPHY

International and Regional Instruments

African Commission on Human and Peoples' Rights, Declaration of Principles on Freedom of Expression and Access to Information in Africa (2019).

African Charter on Human and Peoples' Rights (1981).

African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) (2014).

International Covenant on Civil and Political Rights (1966).

Universal Declaration of Human Rights (1948).

UN Human Rights Committee, General Comment No. 16: Article 17, Right to Privacy (1988).

UN Human Rights Committee, General Comment No. 34: Article 19, Freedoms of Opinion and Expression, CCPR/C/GC/34 (2011).

UN Human Rights Council, Resolution A/HRC/RES/32/13, The Promotion, Protection and Enjoyment of Human Rights on the Internet (2016).

UN Human Rights Council, Resolution A/HRC/RES/51/9, Safety of Journalists (2022).

Council of Europe Committee of Ministers, Recommendation CM/Rec(2024)2 on Countering the Use of Strategic Lawsuits Against Public Participation (SLAPPs) (2024).

Directive (EU) 2024/1069 on Protecting Persons Who Engage in Public Participation from Manifestly Unfounded Claims or Abusive Court Proceedings (2024).

Regulation (EU) 2016/679, General Data Protection Regulation (GDPR).

Zimbabwean Constitutional, Legislative and Policy Materials

Constitution of Zimbabwe Amendment (No. 20) Act, 2013.

Cyber and Data Protection Act [Chapter 12:07].

Freedom of Information Act [Chapter 10:33].

Interception of Communications Act [Chapter 11:20].

Criminal Law (Codification and Reform) Act [Chapter 9:23].

Constitutional Court Rules, 2016.

Criminal Law (Codification and Reform) Act [Chapter 9:23].

Constitutional Court Rules, 2016.

Zimbabwean Case Law

Alistair Michael Fletcher v Minister of Lands, Agriculture, Fisheries, Water and Rural Resettlement & Others CCZ 7/24.

Blessed Mhlanga v Magistrate Nduna N.O. & Others HH 584/21.

Chimakire & Others v Attorney-General of Zimbabwe CCZ 6/14.

Dudzai Mureyi v Health Professions Authority of Zimbabwe and Others HH 823/17, HC 8602/16.

Joseph Mwoyounotsva v Zimbabwe National Water Authority CCZ 9/20.

Mudzuru v Minister of Justice, Legal and Parliamentary Affairs CCZ 12/15.

Mushunje v Zimbabwe Newspapers (1980) Ltd HH 47/17.

Namatai Kwekwedza v Judicial Service Commission & Another HH 140/22.

Posts and Telecommunications Corporation v Modus Publications (Pvt) Ltd 1997 (2) ZLR 492 (S).

Rita Marque Mbatha v Confederation of Zimbabwe Industries and The Sheriff of Zimbabwe CCZ 13/20.

Rusape Town Council v Takudzwa Noel Mwashaenyi & Sheriff of the High Court N.O. HCMTC 70/25; HCMTJ 39/25.

Zimbabwe Lawyers for Human Rights and Media Institute of Southern Africa-Zimbabwe v Minister of State for National Security and Others, High Court of Zimbabwe, 2019.

Zimbabwe Online Content Creators Trust v Zimbabwe Media Commission HH 359/20.

ZANU PF v Zimbabwe Electoral Commission & Another HH 379/18.

Compendium of Case Law Relating to Digital Freedoms | Page Comparative and International Case Law

Ahmet Yildirim v Turkey App no 3111/10 (ECtHR, 18 December 2012).

Axel Springer AG v Germany App no 39954/08 (ECtHR, Grand Chamber, 7 February 2012).

Biancardi v Italy App no 77419/16 (ECtHR, 25 November 2021).

Big Brother Watch and Others v United Kingdom Apps nos 58170/13, 62322/14 and 24960/15 (ECtHR, Grand Chamber, 25 May 2021).

Blind SA v Minister of Trade, Industry and Competition and Others (CCT 320/21) [2022] ZACC 33.

Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems Case C-311/18 (CJEU, 16 July 2020).

Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others Joined Cases C-293/12 and C-594/12 (CJEU, 8 April 2014).

Escher and Others v Brazil, Inter-American Court of Human Rights, Judgment of 6 July 2009.

Google Spain SL and Google Inc. v Agencia Española de Protección de Datos and Mario Costeja González Case C-131/12 (CJEU, 13 May 2014).

Hurbain v Belgium App no 57292/16 (ECtHR, Grand Chamber, 4 July 2023).

McIntyre v Ohio Elections Commission 514 US 334 (1995).

Mineral Sands Resources (Pty) Ltd and Others v Reddell and Others; Mineral Commodities Ltd and Another v Dlamini and Another (CCT 67/22) [2022] ZACC 38.

Mosley v United Kingdom App no 48009/08 (ECtHR, 10 May 2011).

NT1 & NT2 v Google LLC [2018] EWHC 799 (QB).

President of the Republic of South Africa and Others v M & G Media Ltd (CCT 03/11) [2011] ZACC 32; 2012 (2) SA 50 (CC).

Roman Zakharov v Russia App no 47143/06 (ECtHR, Grand Chamber, 4 December 2015).

Thembi-Mahanyele v Mail & Guardian Ltd and Another 2004 (6) SA 329 (SCA).

Tristán Donoso v Panama, Inter-American Court of Human Rights, Judgment of 27 January 2009.

Uuter Dery and Others v Ghana, ECOWAS Court of Justice.

Produced with support from

BERTHA FOUNDATION