LitNet Akademies Jaargang 23, Nommer 2, 2026, ISSN 1995-5928
https://doi.org/10.56273/1995-5928/2026/j23n2e5

Die beperkings van toestemming in die Suid-Afrikaanse inligtingsbeskermingsreg

Gretchen Jansen

Gretchen Jansen, Departement Handelsreg, Universiteit Stellenbosch

Opsomming

In hierdie artikel ondersoek ek die rol en praktiese doeltreffendheid van toestemming binne die Suid-Afrikaanse inligtingsbeskermingsraamwerk onder die Wet op Beskerming van Persoonlike Inligting 4 van 2013. Die vraag word gestel of toestemming, soos gedefinieer en geoperasionaliseer in die Wet, datasubjekte in staat stel om op ’n betekenisvolle wyse beheer oor hul persoonlike inligting uit te oefen. Verder word daar ook gevra of die regulatoriese betekenis daarvan oorskat word in die lig van kognitiewe en strukturele beperkings. Alhoewel Suid-Afrikaanse inligtingsbeskermingswetgewing gegrond is op die waardes van outonomie, waardigheid en selfbeskikking, word twyfel uitgespreek of toestemming hierdie rol in die land se hedendaagse digitale omgewing realisties kan vervul.

Die artikel neem ’n sistematiese regsontleding en sosiotegniese teoretiese raamwerk aan. Dit steun op Suid-Afrikaanse grondwetlike regspraak en die historiese ontwikkeling van die Wet op Beskerming van Persoonlike Inligting – veral die Suid-Afrikaanse Regshervormingskommissie se opvatting van privaatheid as iets wat individuele agentskap oor persoonlike inligting moontlik maak. Hierdie normatiewe grondslag word ondersoek aan die hand van insigte uit die gedragsbesluitnemingsteorie, insluitend begrensde rasionaliteit, heuristieke, verstekvooroordeel en toestemmingsafmatting (“decision fatigue”) om te bepaal of individue in die praktyk in staat is om betekenisvolle inligtingsbeheer uit te oefen. Die ontleding word verder geplaas binne Suid-Afrika se sosiotegnologiese konteks, wat gekenmerk word deur digitale ongelykheid, ongelyke digitale geletterdheid, platformafhanklikheid en die toenemende datafikasie van openbare en private dienste. Dit ontleed die toestemmingsbepalings van die Wet op Beskerming van Persoonlike Inligting, hul normatiewe grondslag en hul praktiese werking in konteks.

https://doi.org/10.56273/1995-5928/2026/j23n2e5

Daar word bevind dat alhoewel die Wet se toestemmingsraamwerk begripsmatig belyn is met grondwetlike waardes, kognitiewe beperkings en strukturele omstandighede die praktiese doeltreffendheid daarvan ondermyn. As gevolg hiervan funksioneer toestemming dikwels as ’n formele regsmeganisme eerder as ’n betekenisvolle uitdrukking van individuele agentskap. Daar word tot die gevolgtrekking gekom dat inligtingsbeskerming in Suid-Afrika minder op individuele toestemming moet staatmaak en eerder institusionele aanspreeklikheid, sterker afdwinging en strukturele beskermings moet prioritiseer om datasubjekte meer effektief te beskerm.

Trefwoorde: digitale bestuur; digitale ongelykheid; gedragsbesluitneming; inligtingsbeskermingsreg; inligtingselfbeskikking; inligtingsprivaatheid; regmatige grondslag vir prosessering; toestemming; Wet op Beskerming van Persoonlike Inligting

Abstract

The limits of consent in South African data protection law

The Protection of Personal Information Act 4 of 2013 (POPIA) represents South Africa’s primary legislative framework for the protection of personal information and gives effect to the constitutional right to privacy. Although POPIA recognises several lawful grounds for processing personal information, consent has assumed a particularly prominent role in both public discourse and organisational compliance practices. Consent is often portrayed as the central mechanism through which individuals exercise control over their personal information and safeguard their privacy interests. This article questions that assumption. It argues that while consent occupies an important place within POPIA’s normative framework, its practical ability to protect data subjects is significantly constrained by both cognitive limitations and the socio-technical realities of contemporary South African digital life.

The article begins by examining the historical and conceptual foundations of POPIA’s consent framework. It traces the origins of the legislation to the South African Law Reform Commission (SALRC) Project 124 on Privacy and Data Protection and demonstrates how the Commission drew heavily on constitutional jurisprudence that linked privacy to autonomy, dignity, and self-determination. Consent emerged within this framework as a mechanism through which informational self-determination could be exercised. At the same time, the SALRC recognised that privacy is not absolute and must be balanced against competing public and private interests.

The article demonstrates that POPIA’s approach to consent was strongly influenced by international data protection instruments, particularly the 1981 Organisation for Economic Cooperation and Development’s Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data, the Council of Europe 1980 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, and the European Union Data Protection Directive 95/46/EC. As a result, POPIA inherited many of the assumptions underlying earlier European data protection models, including the belief that individuals are capable of exercising meaningful control over personal information through informed decision-making. While these assumptions were already being questioned internationally by the time POPIA was enacted, they remain embedded within South Africa’s legislative framework.

https://doi.org/10.56273/1995-5928/2026/j23n2e5

This study then undertakes a doctrinal analysis of POPIA's consent provisions. Section 11 identifies consent as one of several lawful grounds for processing personal information, alongside contractual necessity, legal obligations, legitimate interests, and public law duties. POPIA defines consent as a "voluntary, specific and informed expression of will" through which permission is granted for processing. Although the definition appears conceptually robust, each of its constituent requirements rest on assumptions that become increasingly difficult to sustain in modern digital environments.

A voluntary act requires that individuals have genuine freedom to refuse consent without suffering detriment. Specificity requires consent to relate to clearly defined processing purposes. Informed consent presupposes that individuals understand what they are agreeing to, while the requirement of an expression of will demands some affirmative indication of agreement. The article demonstrates that these requirements mirror international standards and reflect a strong commitment to informational autonomy. However, it argues that the practical conditions necessary to achieve these ideals are frequently absent.

The first major challenge identified by the article arises from cognitive and behavioural limitations. Drawing on behavioural decision-making literature, the article argues that POPIA's consent model assumes an idealised version of human decision-making that does not reflect how individuals actually interact with digital technologies. Individuals operate under conditions of bounded rationality, characterised by limited time, attention, and cognitive capacity. Modern data processing practices are highly complex, often involving secondary uses of data, algorithmic decision-making, cross-border transfers, and opaque processing eco-systems that are difficult even for sophisticated users to understand.

Faced with these complexities, individuals rely on heuristics and cognitive shortcuts rather than careful deliberation. Decisions about privacy are frequently influenced by factors such as brand familiarity, institutional trust, or perceived convenience rather than detailed assessments of data processing practices. The article argues that these behavioural realities undermine the assumption that consent reliably reflects informed and autonomous choice.

These problems are compounded by consent fatigue. Individuals encounter countless consent requests across digital platforms and services. Repeated exposure to consent notices encour-ages habituation and disengagement, leading users to accept requests automatically rather than evaluate them critically. In such circumstances, consent becomes a routine procedural act rather than a meaningful exercise of self-determination.

The article further highlights the role of behavioural influences such as default settings and choice architecture. Digital interfaces are frequently designed in ways that steer users toward acceptance through prominent "accept" options, complex refusal processes, and strategically structured interfaces. Although users technically retain the ability to refuse consent, the architecture of decision-making environments strongly encourages acceptance. Consequently, formal legal choice often masks substantial behavioural manipulation.

The second major challenge explored by the article concerns the structural realities of the South African digital environment. The effectiveness of consent depends on individuals possessing meaningful alternatives and genuine bargaining power. However, South Africa's socio-economic conditions often undermine these prerequisites.

https://doi.org/10.56273/1995-5928/2026/j23n2e5

Persistent digital inequality remains a defining feature of South African society. While internet penetration has increased significantly, substantial disparities remain in access, affordability, digital literacy, and quality of connectivity. Many individuals rely exclusively on mobile internet access and operate within resource-constrained environments where engaging with lengthy privacy disclosures is impractical. Digital literacy deficits further weaken the ability of individuals to understand and evaluate data processing practices.

The article also examines growing platform dependency. Access to communication, employment opportunities, education, commerce, and social participation increasingly depends on a small number of dominant digital platforms. For many users, participation in digital life requires accepting extensive data collection practices. In these circumstances, refusal is often not a realistic option. Consent becomes formally available but substantively meaningless because declining processing may effectively exclude individuals from essential social and economic activities.

State datafication presents an additional challenge. The article highlights the increasing use of biometric systems, digital identity verification, and data-driven public administration within South Africa. Access to welfare benefits, public services, financial products, and identity verification increasingly requires the surrender of personal information. Here, consent becomes particularly problematic because individuals cannot realistically opt out without forfeiting access to essential services. While POPIA contains alternative lawful grounds that better justify such processing, the continued dominance of consent discourse obscures the reality that many forms of data processing are effectively unavoidable.

Against this backdrop, the article argues that consent should no longer be viewed as the primary safeguard within South African data protection law. Instead, greater emphasis should be placed on institutional accountability, transparency, and structural regulation. POPIA already contains a comprehensive accountability framework, including obligations relating to purpose limitation, information quality, security safeguards, openness, and data subject participation. However, the effectiveness of these mechanisms depends on robust enforcement and institutional oversight.

The article concludes that South Africa's data protection framework would be strengthened by shifting its regulatory focus away from individualised consent and toward stronger accountability obligations on responsible parties. This includes enhancing the capacity of the Information Regulator, improving transparency mechanisms, and ensuring meaningful enforcement of existing legal duties. Consent should remain available where genuine choice exists, but it should be regarded as a supplementary safeguard rather than the central mechanism through which privacy and informational self-determination are protected. Such an approach would better reflect the realities of contemporary digital life and more effectively advance the constitutional values that underpin South African data protection law.

Keywords: behavioural decision-making; consent; data protection law; digital governance; digital inequality; information privacy; informational self-determination; lawful basis for processing; Protection of Personal Information Act (POPIA)

https://doi.org/10.56273/1995-5928/2026/j23n2e5

1. Inleiding

Die Suid-Afrikaanse Wet op Beskerming van Persoonlike Inligting 4 van 2013 ("die Wet") beliggaam 'n moderne, beginselsgebaseerde benadering tot inligtingsbeskerming. Alhoewel die Wet verskeie grondslae bied vir regmatige prosessering van persoonlike inligting, het toestemming 'n buitensporige plek in sowel die openbare diskoers as die organisatoriese praktyk ingeneem.[1] Dit weerspieël 'n breër wanopvatting dat toestemming die primêre of standaardregverdiging vir prosessering is. In die praktyk word digitale lewe egter gekenmerk deur sistemiese, infrastrukturele en effektief onvermydelike vorme van inligtingsprosessering. Persoonlike inligting vloei voortdurend deur komplekse tegnologiese en burokratiese stelsels waarmee individue omgaan om toegang te kry tot dienste wat noodsaaklik is vir die moderne alledaagse lewe, soos mobiele netwerke, finansiële bemiddelaars, staatsbeheerde welsyns-tegnologieë, of sosialemediaplatforms. Hierdie werklikheid ontbloot 'n groeiende spanning binne die toestemmingsraamwerk van die Wet op Beskerming van Persoonlike Inligting wat vrywilligheid, ingeligte keuse en 'n mate van gebruikersoutonomie veronderstel wat nie ooreenstem met hoe digitale infrastrukture funksioneer nie.

Individue[2] gebruik toestemmingsmeganismes nie as volkome rasionele besluitnemers wat in staat is om elke versoek om persoonlike inligting sorgvuldig te evalueer nie. Besluite oor die vraag of inligtingsprosessering aanvaar of geweier moet word, word dikwels eerder geneem onder toestande van beperkte aandag, tydsdruk en inligtingsoorlading. Gedragsnavorsing toon dat individue staatmaak op kognitiewe kortpaaie, of heuristieke, wanneer hulle komplekse digitale omgewings navigeer. Verstekvooroordeel, gewoonte aan herhaalde toestemmings-opdragte en toestemmingsafmatting ("decision fatigue") kan alles beïnvloed hoe keuses gemaak word, wat dikwels vinnige aanvaarding eerder as reflektiewe besluitneming aanmoedig. Hierdie dinamika skakel nie noodwendig individuele agentskap uit nie, maar dit bemoeilik die aanname dat toestemming 'n vrywillige, bepaalde en ingeligte wilsuitdrukking betroubaar weerspieël.

In die Suid-Afrikaanse konteks kan die beperkings van toestemming nie verstaan word sonder om inligtingspraktyke binne 'n breër stel strukturele realiteite te plaas nie. Diep sosio-ekonomiese ongelykheid vorm die wyse waarvolgens individue met digitale tegnologieë omgaan. Gemarginaliseerde gemeenskappe is dikwels beperk in hul keuse oor die platforms en stelsels wat hulle kan gebruik om toegang tot werk, kommunikasie of openbare dienste te verkry.[3] Dit word vererger deur groeiende digitale afhanklikheid waar mobiele toestelle en platformgebaseerde dienste as noodsaaklike toegangspunte tot ekonomiese en sosiale deel-name funksioneer.[4] Staatstelsels word toenemend gedatafiseer, wat wissel van biometriese identifikasie en administrasie van maatskaplike toelaes[5] tot polisiëringstegnologieë.[6] Onder hierdie omstandighede word van individue vereis om hul persoonlike inligting te deel ten einde basiese dienste te ontvang. Onderliggend aan hierdie dinamika is die oorheersing van wêreldwye private platforms, hoofsaaklik gebaseer in die Globale Noorde, wat in 'n posisie is om inligtingsbepalings of -voorwaardes eensydig te stel, om met beperkte deursigtigheid te funksioneer, en wat deur buitelandse regsraamwerke gereguleer word.[7] Hierdie strukturele omstandighede vorm die empiriese agtergrond waarteen die Wet op Beskerming van Persoonlike Inligting se toestemmingsraamwerk werk. Dit beklemtoon 'n konteks waarin individue, ondanks die regsvermoede van outonomie, nie realisties kan onderhandel, of die prosessering van hul persoonlike inligting kan weier nie.

https://doi.org/10.56273/1995-5928/2026/j23n2e5

Teen hierdie agtergrond voer ek in hierdie artikel aan dat toestemming as regverdiging vir die prosessering van persoonlike inligting nie as die primêre grondslag vir inligtingsbeskerming in Suid-Afrika kan dien nie. Toestemming veronderstel vrywilligheid, digitale geletterdheid en die realistiese vermoë om te weier, wat omstandighede is wat sistemies ondermyn word deur die bovermelde strukturele realiteite. In die konteks van sosio-ekonomiese ongelykheid, infrastruktuurafhanklikheid en ondeursigtige staatsdatastelsels word toestemming minder 'n vrywillige wilsuitdrukking, en 'n meer formalistiese gebaar wat geen werklike funksie dien om individue se persoonlike inligting en privaatheid te beskerm nie. Die reg se klem op individuele besluitneming verdoesel die feit dat inligtingspraktyke gedryf word deur institusionele, infrastrukturele en geopolitieke kragte wat individue nie betekenisvol kan beïnvloed nie.

Alhoewel daar toenemend navorsing is wat verband hou met die Wet op Beskerming van Persoonlike Inligting en Suid-Afrikaanse inligtingsbeskermingreg, fokus die meeste ontledings op leerstellige interpretasie, afdwinging en belyning met internasionale standaarde.[8] Wêreldwyd het die debat oor toestemming as 'n hoeksteen van inligtingsoutonomie en selfbeskikking in die inligtingsbeskermingsreg al meer aandag begin geniet.[9] Daar is egter min navorsing wat direk die kruispunt ondersoek tussen die Suid-Afrikaanse regsleer oor toestemming as regverdiging vir die prosessering van persoonlike inligting en die strukturele en kontekstuele realiteite soos ongelykheid, infrastruktuurafhanklikheid en beperkte digitale geletterdheid. Die doel van hierdie artikel is om die Wet op Beskerming van Persoonlike Inligting se toestemmingsraamwerk binne die materiële realiteite van die Suid-Afrikaanse digitale lewe te plaas.

Die artikel verloop soos volg: In onderafdeling 2 ondersoek ek die Wet op Beskerming van Persoonlike Inligting se raamwerk vir die regverdiging van die prosessering van persoonlike inligting, met spesifieke fokus op toestemming as regverdiging en die aannames waarop dit berus. In onderafdeling 3 oorweeg ek die vraag hoe kognitiewe en gedragsbeperkings, soos heuristieke, toestemmingsafmatting, verstekvooroordeel en keuse-argitekture die vrywilligheid en ingeligtheid wat vir geldige toestemming vereis word, ondermyn. Onderafdeling 4 demonstreer verder hoe Suid-Afrikaanse kontekstuele realiteite, insluitend digitale geletterdheid, platformafhanklikheid en staatsdatafisering, die vrywilligheid en ingeligtheid wat vir geldige toestemming vereis word, ondermyn en dit grootliks simbolies maak. Laastens word daar, in onderafdeling 5, besin oor die implikasies van hierdie bevindings vir reg en beleid en word daar gepleit vir hervormings wat gerig is op kollektiewe, deursigtigheidsgebaseerde aanspreeklikheid teenoor verantwoordelike partye, eerder as geïndividualiseerde toestemming.

2. Die Wet op Beskerming van Persoonlike Inligting se toestemmingsraamwerk

2.1 Historiese grondslae van die Wet op Beskerming van Persoonlike Inligting se benadering tot toestemming

Die begripsmatige grondslag van die Wet op Beskerming van Persoonlike Inligting se benadering tot toestemming kan teruggevoer word na die Suid-Afrikaanse Regshervormingskommissie se Projek 124 oor Privaatheid en Databeskerming. Die kommissie se werk, wat uiteindelik aanleiding gegee het tot die 2009-verslag, was die eerste volgehoue poging om 'n wetgewende raamwerk vir inligtingsbeskerming in Suid-Afrika te vestig.[10] Uit die staanspoor het die verslag beklemtoon dat enige toekomstige inligtingsbeskermingswetgewing praktiese effek moes gee aan die reg op privaatheid, soos beskerm deur die gemenereg en vervat in

https://doi.org/10.56273/1995-5928/2026/j23n2e5

artikel 14 van die Grondwet van Suid-Afrika.[11] Die verslag het sleutelbesluite van die Konstitusionele Hof en die Hoogste Hof van Appèl ontleed om te illustreer hoe privaatheid in die Suid-Afrikaanse reg gekoppel is aan waardes soos individuele outonomie, waardigheid en selfbeskikking.[12]

Die Kommissie verwys na *Bernstein v Bester* 1996 2 SA 751 (KH), waar regter Ackermann die idee van ’n “kontinuum” van privaatheid verwoord het: Hoe meer ’n persoon in gemeenskaplike of openbare ruimtes beweeg, hoe nouer is die omvang van privaatheidsbeskerming. Die kommissie herlei uit *Bernstein* nie net ’n ruimtelike konsep van privaatheid nie, maar ’n normatiewe een: Privaatheid beskerm die omstandighede waaronder individue ’n outonome keuse kan ontwikkel en uitoefen.[13] Die erkende “kontinuum” van privaatheid weerspieël die idee dat outonomie die sterkste is in die intieme sfeer, alhoewel dit nie heeltemal uitgeskakel is in kommersiële of openbare kontekste nie. Hierdie siening is verder erken deur regter Langa in *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd; In re Hyundai Motor Distributors (Pty) Ltd v Smit* 2001 1 SA 545 (KH).[14] Hieruit beklemtoon die verslag dat inligtings- en ruimtelike privaatheid verweef is en dat enige indringing aan die grondwetlike standaarde van redelikheid en proporsionaliteit moet voldoen. Die klem op regverdiging weerspieël die begrip dat privaatheid, hoewel fundamenteel vir waardigheid en selfbeskikking, nie absoluut is nie en gebalanseer moet word teen mededingende gemeenskapsbelange.[15]

Die kommissie se steun op *National Media Ltd v Jooste* 1996 3 SA 262 (HHA) illustreer die gemeneregtelike beskerming teen die onregmatige publikasie van private feite. Hier word privaatheid gestel as ’n aspek van persoonlikheid wat beskerming verdien omdat ongemagtigde openbaarmaking individuele waardigheid en die vermoë om mens se openbare identiteit te beheer, ondermyn. Die kommissie beskou hierdie ontwikkeling as bewys dat die Suid-Afrikaanse reg reeds begin het om inligtingselfbeskikking[16] binne die *actio iniuriarum* te erken, selfs voor die bestaan van omvattende inligtingsbeskermingswetgewing.[17]

Die verslag steun verder op *NM v Smith* 2007 5 SA 250 (KH) wat handel oor die publikasie van ’n individu se MIV-status sonder toestemming. Die kommissie herlei uit *NM* die beginsel dat beheer oor persoonlike inligting, veral sensitiewe inligting, sentraal staan tot die beskerming van individue se morele agentskap en selfbeskikking. Die skade het nie net in blootstelling gelê nie, maar ook in die ontneming van die individu se vermoë om te besluit wanneer, hoe en aan wie sodanige inligting bekend gemaak sou word.[18] Die hof se erkenning dat die ongemagtigde openbaarmaking van sensitiewe mediese inligting ’n ernstige skending van waardigheid uitmaak, word as besonder belangrik beskou vir die latere regulering van “spesiale persoonlike inligting”.[19] Verder verwys die kommissie ook na *Mistry v Interim National Medical and Dental Council of South Africa* 1998 4 SA 1127 (KH) om te illustreer dat privaatheid nie absoluut is nie en in regulatoriese kontekste beperk kan word, maar slegs onder grondwetlike waarborge.[20]

Dit is teen hierdie regskundige agtergrond dat die kommissie toestemming beskou as ’n meganisme waardeur individue beheer oor hul persoonlike inligting kan uitoefen.[21] Terselfdertyd het die kommissie beklemtoon dat privaatheid nie ’n absolute reg is nie: Sowel die Grondwet as die gemenereg vereis dat privaatheidsbelange gebalanseer word teen mededingende regte en regmatige openbare of private belange. Die aanbevelings noem dat inligtingsbeskerming hierdie dubbele aard van privaatheid moet weerspieël: Dit moet beskermend wees vir individuele agentskap, maar terselfdertyd inherent onderhewig aan kontekstuele beperkings.[22] Dit

https://doi.org/10.56273/1995-5928/2026/j23n2e5

het ook die opvatting beïnvloed dat toestemming nie die enigste meganisme is om prosessering te regverdig nie, maar eerder ’n belangrike regsuitdrukking van inligtingsoutonomie is wat funksioneer binne ’n raamwerk wat onderworpe is aan mededingende magsdinamika, beleidsoorwegings en strukturele beperkings. Hierdie leerstellige grondslag word later van deurslaggewende belang in die ondersoek waarom toestemming, soos dit uiteindelik in die Wet op Beskerming van Persoonlike Inligting gekodifiseer is, sukkel om as ’n doeltreffende waarborg te funksioneer om uitvoering te gee aan die reg op privaatheid, soos voorgestel.

Verder beklemtoon die verslag herhaaldelik die behoefte dat Suid-Afrika homself met internasionale standaarde moet belyn om inligtingsvloei oor landsgrense te fasiliteer en regsekerheid vir besighede te verbeter.[23] In hierdie verband het die kommissie op drie belangrike internasionale instrumente staatgemaak:

1. Die Raad van Europa se 1981-Konvensie vir die beskerming van individue met betrekking tot die outomatiese prosessering van persoonlike data.[24]
2. Die Organisasie vir Ekonomiese Samewerking en Ontwikkeling (OESO) se 1981-Riglyne wat die beskerming van privaatheid en datavloei oor landsgrense van persoonlike data reguleer.[25]
3. Die Europese Unie se Databeskermingsriglyn van 1995.[26]

Destyds is die Databeskermingsriglyn beskou as die internasionale goue standaard vir inligtingsbeskerming, aangesien dit die omvattendste wetgewende raamwerk oor die saak verskaf het.[27] Teen die tyd dat die wetgewende proses vir die Wet op Beskerming van Persoonlike Inligting in 2013 afgehandel was, was die Europese Unie se Algemene Regulasie oor Databeskerming 2016/679[28] nog nie aangeneem nie. Om hierdie rede weerspieël baie van die bepalings in die Wet op Beskerming van Persoonlike Inligting, soos verorden, dié in die Databeskermingsriglyn.[29] As gevolg hiervan het die Wet baie van die Databeskermingsriglyn se onderliggende aannames rakende toestemming as regverdiging vir die prosessering van persoonlike inligting geërf.

Ten einde hierdie genealogie te verstaan, is dit van kardinale belang om die Wet op Beskerming van Persoonlike Inligting se toestemmingsbepalings, soos verorden, te ondersoek. Die Wet se fokus op toestemming weerspieël beide die kommissie se interpretasie van die reg op privaatheid en sy begeerte om Suid-Afrikaanse wetgewing met globale norme te belyn. Dit beteken egter ook dat die Wet se model deur die beperkings van die Databeskermingsriglyn-era gevorm is – beperkings wat later met die aanneming van die Algemene Regulasie oor Databeskerming aangespreek en opgelos is.

2.2 Die Wet op Beskerming van Persoonlike Inligting se toestemmingsraamwerk: teoretiese oorsig

Die Wet op Beskerming van Persoonlike Inligting neem ’n beginselgebaseerde regulatoriese model aan wat in ooreenstemming is met die internasionale inligtingsbeskermingstandaarde wat in die OESO-riglyne en die Databeskermingsriglyn gestel is. Die aanhef omskryf die Wet as die uitvoering van die grondwetlike reg op privaatheid. Daar word verder erken dat dit beperk kan word deur “regverdigbare beperkings wat daarop gemik is om ander regte en belangrike belange te beskerm”, asook om die vrye vloei van inligting, plaaslik en oor grense heen, te fasiliteer met die doel om ekonomiese en sosiale vooruitgang “binne die raamwerk van die inligtingsamelewing” te bevorder.[30] Die Wet probeer individuele beskerming balanseer

https://doi.org/10.56273/1995-5928/2026/j23n2e5

met ekonomiese en administratiewe doeltreffendheid deur breë, buigsame beginsels, eerder as voorskriftelike reëls te gebruik. Dit blyk ook uit die begrip van toestemming: Dit is een grondslag vir regmatige prosessering binne 'n stelsel wat veronderstel dat verantwoordelike partye die beginsels in konteks sal operasionaliseer.

Die regmatige prosessering van persoonlike inligting onder die Wet op Beskerming van Persoonlike Inligting is rondom agt voorwaardes gestruktureer: verantwoordingspligtigheid, beperkte prosessering, oogmerkspesifikasie, beperkte verdere prosessering, inligtingsgehalte, openheid, veiligheidsvoorsorgmaatreëls en deelname deur die datasubjek.[31] Hierdie voorwaardes vereis dat verantwoordelike partye prosessering regverdig en beperk, deursigtigheid verseker en prosedurele waarborge handhaaf. Dit is die grondslag van die Wet, terwyl die grondslag vir regmatige prosessering, insluitend toestemming, binne voorwaarde twee (beperkte prosessering) val as meganismes om te verseker dat die prosessering van persoonlike inligting binne die grense van die reg plaasvind.

Binne hierdie raamwerk bepaal artikel 11 van die Wet dat persoonlike inligting geprosesseer mag word slegs (i) indien die datasubjek toestemming daarvoor gee; (ii) wanneer dit noodsaaklik is om 'n kontrak uit te voer; (iii) om aan 'n verpligting wat deur die reg opgelê is, te voldoen; (iv) om 'n regmatige belang van die datasubjek te beskerm; (v) wanneer dit noodsaaklik is om 'n openbare regsplig uit te voer; (vi) om die regmatige belange van die verantwoordelike party of 'n derde party na te streef.[32] Alhoewel toestemming eerste gelys word, is dit nie die bedoeling van die Wet (soos die Databeskermingsriglyn) dat dit die standaard of mees toepaslike grondslag vir regmatige prosessering in alle omstandighede moet wees nie.[33] In die Suid-Afrikaanse openbare diskoers en praktyk word toestemming egter dikwels as die sentrale regverdiging beskou, wat die ongewenste volharding van kennis-en-keuse-narratiewe weerspieël.[34]

Die Wet op Beskerming van Persoonlike Inligting definieer in artikel 1 toestemming as "enige vrywillige, bepaalde en ingeligte wilsuitdrukking waarvan verlof tot die prosessering van persoonlike inligting gegee word".[35] Uit hierdie definisie kan vier elemente geïdentifiseer word wat gesamentlik 'n relatief hoë drempel stel, breedweg in ooreenstemming met die Databeskermingsriglyn se vereiste dat toestemming "vrywillig, bepaald en ingelig" moet wees.[36] Die Algemene Regulasie oor Databeskerming het later "ondubbelsinnig" en "duidelike bevestigende handeling" as vereistes bygevoeg,[37] maar die onderliggende logika bly dieselfde: Geldige toestemming vereis duidelikheid van oogmerk, voldoende openbaarmaking en die egte vermoë om toestemming te weier.

Die vier elemente van vrywilligheid, bepaaldheid, ingeligtheid en wilsuitdrukking word nie in die Wet gedefinieer nie en vereis noukeuriger ondersoek. Alhoewel hierdie aspekte nog nie in 'n geregshof bespreek is nie, is daar in navorsing vasgestel dat die begrip van hierdie konsepte ingegee kan word deur die gevestigde beginsels rakende die ekwivalente vereistes in die Databeskermingsriglyn en die Algemene Regulasie oor Databeskerming.[38]

Vrywilligheid is die mees betwiste element. Toestemming kan as vrywillig beskou word slegs as datasubjekte 'n vrye keuse het en later hul toestemming sonder nadeel kan terugtrek.[39] Daarom kan die toestemming nie deur dwang, misleiding of druk verkry word nie.[40] Soos vasgestel in aanhef 43 van die Algemene Regulasie oor Databeskerming, waar daar 'n magswanbalans tussen die datasubjek en die verantwoordelike party is, sal dit onwaarskynlik wees dat die toestemming vryelik (of vrywillig) gegee word. Verder moet die toestemming nie

https://doi.org/10.56273/1995-5928/2026/j23n2e5

saam met bepalings en voorwaardes gebundel word nie, wat beteken dat die datasubjek die vryheid moet kan behou om toestemming te weerhou, maar steeds die bepalings en voorwaardes kan aanvaar.[41]

Bepaaldheid vereis dat toestemming verband moet hou met ’n spesifieke en duidelik gedefinieerde doel. Artikel 13 se oogmerkspesifikasievoorwaarde versterk hierdie vereiste.[42] Omvattende toestemming wat alle doeleindes dek waarvoor persoonlike inligting geprosesseer sou word, sou te vaag wees om geldig te wees.[43] Soos bepaal deur die Europese Databeskermingsraad, moet toestemming “granulêr” wees.[44]

Ingeligte toestemming vereis dat datasubjekte moet verstaan waartoe hulle instem. Die toestemming moet so geformuleer wees dat die datasubjek in ’n posisie geplaas word om ’n ingeligte besluit te neem.[45] Die Wet op Beskerming van Persoonlike Inligting se openheidsvoorwaarde, in artikels 17 en 18 voorsien, is bedoel om dit te ondersteun deur van verantwoordelike partye te vereis om datasubjekte van sleutelinligting in kennis te stel. Dit sluit in: die identiteit van die verantwoordelike party, die inligting wat versamel word en die oogmerk van sodanige versameling, die gevolge van ’n versuim om die inligting te verskaf, en of die inligting aan ’n derde party oorgedra sal word.[46] Anders as die Algemene Regulasie oor Databeskerming, vereis die Wet op Beskerming van Persoonlike Inligting nie dat hierdie inligting in eenvoudige taal verskaf word nie. Daar is egter aangevoer dat die standaard wat in die Suid-Afrikaanse Verbruikersbeskermingswet 68 van 2008 gestel is, insiggewend is.[47] Dit bepaal dat die vervaardiger van ’n kennisgewing wat vereis word ingevolge die Verbruikersbeskermingswet of enige ander wet – soos die Wet op Beskerming van Persoonlike Inligting – die kennisgewing in eenvoudige taal moet verskaf.[48] In hierdie verband sou inligting aan hierdie vereiste voldoen indien “dit redelik is om af te lei dat [van] ’n gewone verbruiker van die klas persone vir wie die [inligting] bedoel is, met gemiddelde geletterdheidsvaardighede en minimale ervaring as verbruiker van die relevante goedere of dienste, verwag kan word om die inhoud, betekenis en belangrikheid van die [inligting] sonder onnodige moeite te verstaan”.[49] Alhoewel hierdie standaard in navorsing vasgestel is, is dit nog nie in ’n geregshof getoets nie; dus, soos dit tans staan, kan verantwoordelike partye formeel daaraan voldoen terwyl hulle steeds digte, ontoeganklike blootleggings verskaf.

Laastens beteken die vereiste van ’n wilsuitdrukking dat toestemming deur ’n bevestigende handeling aangedui moet word. Alhoewel die Wet nie uitdruklik “opt out” of geïmpliseerde toestemmingsmeganismes verbied nie, toon artikel 69, wat op direkte bemarking betrekking het, dat die Wet “opt in” as die verstek in ten minste sommige kontekste beskou. Daar kan aangevoer word dat hierdie meer toegeeflike benadering tot geïmpliseerde toestemming van die Databeskermingsriglyn geërf is. Daar word wel aangevoer dat die oorwegings wat van toepassing is op die Algemene Regulasie oor Databeskerming se “duidelike bevestigende handeling”, toegepas moet word by die interpretasie van hierdie element. Toestemming kan nie by verstek, stilte of onaktiwiteit gegee word nie,[50] en die handeling om toestemming te gee moet verskil van ander handelinge, soos om die bepalings van ’n kontrak te aanvaar.[51]

Alhoewel die Wet op Beskerming van Persoonlike Inligting nie toestemming as die standaardgrondslag vir regmatige prosessering beskou nie, identifiseer die Wet wel spesifieke kontekste waarin toestemming óf vereis, óf verkies word. Direkte bemarking is die duidelikste voorbeeld: Artikel 69 neem ’n “opt in”-model aan, wat direkte bemarking deur middel van ongeoorloofde elektroniese kommunikasie toelaat slegs waar die datasubjek in die voorgeskrewe vorm vooraf toestemming gegee het.[52] Dit volg die logika wat onder die Databeskermingsriglyn toegepas

https://doi.org/10.56273/1995-5928/2026/j23n2e5

was, naamlik dat bemarking ’n verhoogde risiko van indringing en manipulasie inhou en dat individuele keuse as ’n beskermende drempel moet funksioneer.[53]

Net so heg die Wet op Beskerming van Persoonlike Inligting groter waarde aan toestemming wanneer dit handel oor spesiale persoonlike inligting (artikels 26 tot 33) en persoonlike inligting van kinders (artikels 34 en 35). In hierdie areas word toestemming nie net as ’n regsgrondslag beskou nie, maar beklemtoon dit ook die idee dat sekere kategorieë inligtingwaardigheid, diskriminasierisiko of ongelyke magsverhoudings in so ’n mate raak dat dit verhoogde individuele beheer regverdig. Hierdie gebiede van toestemmingsgebaseerde beskerming illustreer die breër teoretiese aanname dat individuele agentskap, uitgeoefen deur toestemming, inligtingsprosesseringsrisiko’s betekenisvol kan versag. Dit beklemtoon ook die spanning in die kern van die Wet op Beskerming van Persoonlike Inligting se toestemmingsmodel: Die kontekste waarin die Wet die sterkste op toestemming steun, is juis dié waar betekenisvolle keuse in die praktyk die minste haalbaar is.

In die geheel beskou, is die Wet op Beskerming van Persoonlike Inligting se definisie van toestemming konseptueel kragtig, maar in die praktyk kan dit operasioneel beperk wees. Dit is gegrond op ’n regsraamwerk wat stabiele en verstaanbare verhoudings tussen datasubjekte en verantwoordelike partye veronderstel. Soos daar in die volgende afdelings aangetoon word, word hierdie aanname onder druk geplaas deur die kognitiewe en gedragsomstandighede waaronder individue met toestemmingsmeganismes omgaan, asook die breër strukturele realiteite van die Suid-Afrikaanse sosiotegniese omgewing.

3. Kognitiewe en gedragsbeperkings op toestemming

Die Wet op Beskerming van Persoonlike Inligting se toestemmingsraamwerk berus op die uitgangspunt dat individuele datasubjekte in staat is om betekenisvolle, outonome besluite te neem oor die prosessering van hul persoonlike inligting. Die statutêre definisie vereis dat toestemming ’n vrywillige, bepaalde en ingeligte wilsuitdrukking moet wees. Implisiet in hierdie vereistes is ’n model van die datasubjek as ’n rasionele en aandagtige besluitnemer wat in staat is om met inligting om te gaan, gevolge te evalueer en werklike keuses uit te oefen. ’n Beduidende korpus van navorsing toon egter dat individue tipies nie op hierdie beraadslagende wyse met toestemmingsmeganismes omgaan nie. In plaas daarvan word besluitneming in digitale omgewings gevorm deur kognitiewe kortpaaie, besluitnemingsafmatting, verstekinstellings en gewoontegedrag. Hierdie gedragsdinamika gee nie bloot aanleiding tot die mislukking van toestemming in sekere gevalle nie, maar ondermyn sistematies die voorwaardes wat nodig is vir toestemming om as ’n doeltreffende meganisme van individuele beheer te funksioneer.

3.1 Kognitiewe beperkings op ingeligte en bepaalde toestemming

Die Wet op Beskerming van Persoonlike Inligting se vereiste dat toestemming “ingelig” moet wees, weerspieël die beginsel dat individue die aard en implikasies van die prosessering waartoe hulle instem, moet verstaan. Hierdie vereiste gee regsuitdrukking aan die idee dat individue betekenisvolle beheer oor hul persoonlike inligting kan uitoefen deur ’n bewuste en doelbewuste keuse. Hierdie uitgangspunt veronderstel egter dat individue in staat is om met inligting om te gaan op ’n wyse wat oplettend, evaluerend en vooruitstrewend is. In die praktyk

https://doi.org/10.56273/1995-5928/2026/j23n2e5

vind besluitneming in digitale omgewings plaas onder toestande van begrensde rasionaliteit,[54] waar individue komplekse inligtingsomgewings met beperkte tyd, aandag en kognitiewe hulpbronne moet navigeer.[55]

Die inligtingskompleksiteit van moderne dataprosessering oortref dit wat individue redelikerwys kan begryp. Privaatheidskennisgewings beskryf dikwels tegniese en abstrakte praktyke, soos dataversameling, outomatiese besluitneming, sekondêre gebruike en oordragte oor landsgrense, waarvan die implikasies selfs vir kundige gebruikers moeilik is om te beoordeel. Die toekomstige gebruike en gevolge van persoonlike inligting is dikwels onbepaald ten tyde van versameling, wat betekenisvolle toestemmingsevaluering verder bemoeilik. Alhoewel die Wet vereis dat individue ingelig moet word oor die oogmerk en omvang van die prosessering,[56] verseker die formele bepalings van inligting nie die praktiese verstaanbaarheid daarvan nie. As gevolg hiervan kan die regsgeldigheid van toestemming deur openbaarmaking verseker word, selfs wanneer individue nie ’n betekenisvolle begrip het van dit waarop hulle ooreengekom het nie. Die aanname dat openbaarmaking alleen inligtingsbeheer moontlik maak, berus daarom op ’n geïdealiseerde model van begrip wat nie die realiteite van digitale interaksie weerspieël nie.

In die lig van hierdie inligtingsvereistes vertrou individue op kognitiewe kortpaaie, of heuristieke, om besluite doeltreffend te neem. In plaas daarvan om die inhoud van inligtingsprosesseringspraktyke sorgvuldig te evalueer, lei individue dikwels betroubaarheid af uit kontekstuele leidrade soos handelsmerkvertroudheid, institusionele legitimiteit of wydverspreide gebruik.[57] Die heuristieke is nie irrasioneel nie; dit is noodsaaklike strategieë wat individue toelaat om te funksioneer in omgewings wat gekenmerk word deur inligtingsoorlading. Dit beteken egter ook dat toestemmingsbesluite dikwels gevorm word deur oënskynlike vertroue en vertroudheid eerder as deur ’n wesenlike beoordeling van prosesseringspraktyke. In hierdie kontekste weerspieël die daad van toestemming ’n algemene ingesteldheid teenoor die diens of instelling, eerder as ’n bepaalde en ingeligte ooreenkoms oor bepaalde vorme van inligtingsprosessering.[58]

Hierdie kognitiewe dinamika het direkte implikasies vir die waardes van outonomie en inligtingselfbeskikking wat die inligtingsbeskermingsreg onderlê. Outonomie veronderstel die vermoë om besluite te neem gebaseer op ’n begrip van relevante inligting, terwyl inligtingselfbeskikking berus op die vermoë om te beheer hoe persoonlike inligting ingesamel en gebruik word. Waar individue nie ’n praktiese begrip van inligtingspraktyke het nie, of op heuristieke staatmaak eerder as oorweging, word hul vermoë om betekenisvolle toestemming uit te oefen, verminder.[59] Toestemming kan as ’n formele aanduiding van instemming funksioneer sonder om die substantiewe outonomie te verseker wat dit bedoel is om te beskerm. Op hierdie wyse verswak die kognitiewe beperkings, wat inherent is aan digitale besluitnemingsomgewings, die verband tussen toestemming en die grondwetlike waardes van waardigheid, outonomie en selfbeskikking waarop Suid-Afrika se inligtingsbeskermingsraamwerk berus.

Hierdie beperkings word verder vererger deur die herhaling waarmee individue in digitale omgewings toestemming moet gee. Herhaalde blootstelling aan toestemmingsversoeke veroorsaak die toestand, alreeds vroeër genoem, wat beskryf word as “toestemmingsafmatting”, waar individue van toestemmingsmeganismes onttrek weens hul alomteenwoordigheid en skynbare onvermydelikheid.[60] Onder sulke omstandighede word toestemming geroetineer eerder as beraadslagend, en funksioneer dit as ’n prosedurele stap wat nodig is om toegang tot ’n diens te kry, eerder as ’n betekenisvolle uitoefening van keuse. Hierdie gedragsaanpassing weerspieël die praktiese onmoontlikheid van volgehoue, aandagtige betrokkenheid by die volume

https://doi.org/10.56273/1995-5928/2026/j23n2e5

en kompleksiteit van toestemmingsinteraksies wat in die hedendaagse digitale lewe ervaar word.

3.2 Gedragsbeperkings op vrywillige toestemming

Benewens kognitiewe beperkings, ondermyn gedragsdinamika verder die aanname dat toestemming onder die Wet op Beskerming van Persoonlike Inligting 'n vrywillige wilsuitdrukking weerspieël. Die Wet vereis dat toestemming vrywillig gegee word. Dit impliseer dat individue dataprosessering moet kan aanvaar of weier sonder dwang, manipulasie of onnodige druk. Hierdie vereiste weerspieël die reg se verbintenis daartoe om individuele outonomie en waardigheid te respekteer deur te verseker dat individue werklike beheer behou oor besluite rakende hul persoonlike inligting. Gedragsnavorsing toon egter dat besluitneming hoogs vatbaar is vir kontekstuele invloede, insluitend verstekinstellings en koppelvlakontwerp, wat uitkomste kan vorm sonder om 'n formele keuse te beperk.[61] Hierdie invloede skakel keuse nie heeltemal uit nie, maar lei individue sistematies na spesifieke besluite op maniere wat die vrywilligheid en legitimiteit van toestemming verswak.

Een van die belangrikste gedragsinvloede spruit uit die krag van verstekinstellings. Individue is geneig om vooraf gekose opsies te aanvaar, nie omdat hulle dit bewustelik geëvalueer en goedgekeur het nie, maar omdat die verandering van standaardinstellings moeite, aandag en selfvertroue verg. Hierdie verskynsel, wat dikwels die "status quo-vooroordeel" genoem word, weerspieël 'n algemene neiging om die weg van die minste weerstand te kies in omstandighede van onsekerheid of kompleksiteit.[62] In digitale omgewings laat verstekinstellings dikwels uitgebreide inligtingsinsameling en -deel toe, wat beteken dat individue kan "aanvaar" bloot deur nie vooraf ingestelde opsies te verander nie. Alhoewel individue die formele vermoë behou om toestemming te weier of te wysig, maak die struktuur van die besluitnemingsomgewing aanvaarding die waarskynlikste uitkoms. In sodanige gevalle weerspieël toestemming gedragstraagheid eerder as 'n doelbewuste en outonome uitoefening van inligtingselfbeskikking.

Die ontwerp van digitale koppelvlakke vorm toestemmingsbesluite verder deur wat dikwels as "keuse-argitekture" beskryf word.[63] Toestemmingsversoeke word tipies aangebied op maniere wat aanvaarding aanmoedig, soos deur prominente "aanvaar alles"-knoppies, gefragmenteerde openbaarmaking, of herhaalde aanwysings wat toegang tot verlangde dienste onderbreek. Hierdie ontwerpskenmerke verwyder nie noodwendig die opsie om toestemming te weier nie, maar verhoog die kognitiewe en praktiese inspanning wat nodig is om dit te doen. Met verloop van tyd leer individue dat weiering ongerieflik, tydrowend of ontwrigtend is, terwyl aanvaarding seepgladde toegang tot digitale dienste moontlik maak. Dit skep 'n omgewing waarin toestemming die standaard gedragsreaksie word, nie omdat individue inligtingsprosesseringspraktyke duidelik goedgekeur het nie, maar omdat aanvaarding die maklikste en doeltreffendste uitweg bied.[64] Die gevolglike toestemming kan dus nie maklik as heeltemal vrywillig gekarakteriseer word nie, selfs al voldoen dit aan die formele regsvereistes.

Saam met die kognitiewe beperkings hier bo bespreek, dui hierdie gedragsbeperkings daarop dat toestemming nie die volle normatiewe gewig kan dra wat daaraan toegeken word binne die Wet op Beskerming van Persoonlike Inligting se regulatoriese raamwerk nie. Ofskoon toestemming steeds 'n belangrike meganisme is om individuele agentskap te erken, word die doeltreffendheid daarvan as 'n hulpmiddel om outonomie, waardigheid en inligtingselfbeskikking te beskerm, aansienlik verswak deur die gedragsrealiteite van digitale besluitneming.

https://doi.org/10.56273/1995-5928/2026/j23n2e5

4. Strukturele beperkings op toestemming in die Suid-Afrikaanse konteks

Toestemming funksioneer as ’n effektiewe waarborg slegs as sekere teoretiese aannames geld, naamlik dat individue kan verstaan wat met hul persoonlike inligting gedoen word, dat hulle betekenisvolle alternatiewe het, en dat die besluit om prosessering te aanvaar of te weier werklike agentskap eerder as strukturele druk weerspieël. Die Wet op Beskerming van Persoonlike Inligting erf hierdie aannames van die breër liberaal-individualistiese tradisie van databeskerming, wat toestemming sien as ’n meganisme waardeur outonome subjekte beheer oor persoonlike inligting uitoefen.[65] Hierdie model veronderstel egter relatief simmetriese mag, duidelike en deursigtige inligtingsvloei, en kontekste waarin die weerhouding van toestemming ’n realistiese opsie is. In die Suid-Afrikaanse sosiotegniese omgewing is dit selde die geval. In plaas daarvan skep diep sosio-ekonomiese ongelykheid, ongelyke digitale geletterdheid, platformafhanklikheid en groeiende staatsdatafikasie omgewings waarin die formele elemente van toestemming – vrywilligheid, bepaaldheid, ingeligte besluitneming en wilsuitdrukking – sistematies belemmer word.

Voortdurende digitale ongelykheid in Suid-Afrika ondermyn wesenlik die vrywilligheid en ingeligtheid wat ’n toestemmingsmodel veronderstel. Konnektiwiteit het eksponensieel gegroei oor die afgelope paar jaar. In 2025 is berig dat sowat 79,6% van die bevolking ’n vorm van internettoegang het,[66] maar dit weerspieël nie die voortdurende ongelykhede in toegang en kapasiteit nie. Alhoewel baie huishoudings nou minstens een lid met ten minste ’n vorm van internettoegang het, het slegs ’n klein fraksie van huishoudings vastelyn- of tuisinternet-verbinding, met mobiele internet verreweg die dominante toegangswyse.[67] Verder bly die digitale kloof vir ’n beduidende minderheid werklik en blywend. Ongeveer 21% van die bevolking – ongeveer 13,6 miljoen mense – is ongekoppeld.[68] Selfs onder diegene wat gekoppel is, verskil kwaliteit skerp. Ongeveer ’n derde van gebruikers is hoofsaaklik afhanklik van mobiele data, wat steeds onbetaalbaar duur is volgens wêreldwye standaarde.[69] Dit beperk die tyd wat mense kan spandeer om platforms te navigeer of privaatheidskennisgewings te lees. Hierdie ongelykhede word direk op sosio-ekonomiese lynstrukture weerspieël, met lae-inkomste-, landelike en informele-nedersetting-gebruikers wat ongelyk in bandbreedtebeperkte, hoëkoste-digitale omgewings funksioneer.[70] In sulke omstandighede is die gedagte dat individue vryelik die bepalings van inligtingsprosessering kan oorweeg en beding, grootliks fiktief.

Gepaardgaande met beperkte opvoeding of digitalevaardigheidstekorte in baie gemeenskappe is die “ingeligte” element van toestemming op sy beste broos. Verskeie studies oor die aanvaarding van inligting-en-kommunikasie-tegnologie (IKT) in landelike of lae-inkomste-Afrikakontekste, insluitend Suid-Afrika, beklemtoon koste, beperkte toestelbeskikbaarheid, gebrek aan digitale-geletterdheidsopleiding en institusionele verwaarlosing as sleutelhindernisse vir effektiewe digitale burgerskap.[71] Wanneer die inligtingsvoorwaardes vir outonome keuse afwesig is, funksioneer toestemming minder as ’n waarborg en meer as ’n prosedurele fiksie wat inligtings-inwinning regverdig. Hierdie realiteite maak die Wet op Beskerming van Persoonlike Inligting se afhanklikheid van individuele toestemming struktureel wansporig met die werklike digitale konteks van ’n groot deel van Suid-Afrika se bevolking.

Hierdie strukturele ongelykhede word vererger deur die feit dat deelname aan die digitale lewe vir baie Suid-Afrikaners nie meer opsioneel is nie. Namate kern- sosiale en ekonomiese funksies aanlyn migreer, raak individue toenemend afhanklik van ’n klein aantal private, hoofsaaklik buitelandse, platforms om toegang tot inligting , werksgeleenthede, kommunikasie-instrumente, regeringsdienste en finansiële produkte te verkry.[72] Toepassings soos WhatsApp het die primêre

https://doi.org/10.56273/1995-5928/2026/j23n2e5

kommunikasiemiddel geword,[73] terwyl platforms soos Facebook, LinkedIn en aanlyn werwingsportale vir die werksoekende jeug onontbeerlik geword het.[74] Toegang tot hierdie ruimtes word toenemend ’n voorvereiste vir betekenisvolle digitale burgerskap.[75]

Hierdie platformafhanklikheid skep ’n magswanbalans wat toestemming formeel beskikbaar, dog inhoudelik leeg maak. Wanneer platforms noodsaaklike toegangspunte tot sosiale deelname is, is weiering van toestemming prakties onmoontlik.[76] Die Wet op Beskerming van Persoonlike Inligting erken dat toestemming nie die enigste regsbasis vir prosessering is nie, en in baie noodsaaklike-diens-kontekste is ander gronde, soos noodsaaklikheid vir dienslewering of nakoming van regsverpligtinge, meer toepaslik. Tog word toestemming in die praktyk steeds as die standaardgrondslag vir prosessering beskou, selfs wanneer die voorwaardes vir geldige toestemming afwesig is. Dit skep die indruk dat individue hulself kan beskerm deur bloot in te stem of te weier, terwyl die meeste gebruikers in werklikheid min invloed het en noodsaaklike platforms nie kan gebruik sonder om omvattende inligtingspraktyke te aanvaar nie.[77] In ’n konteks gevorm deur wêreldwye platformdominansie – dikwels verstaan binne die breër kritiek op digitale kolonialisme[78] – staar Suid-Afrikaanse gebruikers ’n struktureel dwingende omgewing in die gesig waarin toestemming minder as ’n ware uitoefening van outonomie, maar meer as ’n formele vereiste funksioneer, wat die gebrek aan werklike keuse verberg. Dit is nodig om verder as toestemming as ’n sentrale organiseringsbeginsel te beweeg ten einde die Wet op Beskerming van Persoonlike Inligting se inligtingsbeheermodel in ooreenstemming te bring met die omstandighede van die hedendaagse digitale lewe.

’n Ander belangrike faset wat bydra tot die ineenstorting van toestemming, is die bestendige uitbreiding van staatsgedrewe datafisering en die verwewing van openbare en private stelsels van identiteit, welsyn en kontrolering. In Suid-Afrika het die uitrol van biometriese verifikasiestelsels in 2025 skerp versnel: Die Suid-Afrikaanse Maatskaplike Sekerheidsagentskap (SASSA) het onlangs gesigs- en vingerafdruk- biometriese registrasie verpligtend gemaak vir alle nuwe maatskaplike-toelae-aansoekers en bestaande begunstigdes wat hersien word.[79] Verder het die Departement van Binnelandse Sake ’n opgradering van sy nasionale digitale verifikasiestelsel voltooi, wat nou nie net staatsdepartemente nie, maar ook privaatsektorinstansies, soos banke en versekeringsmaatskappye, in staat stel om identiteite teen die Nasionale Bevolkingsregister te verifieer met behulp van biometriese inligting.[80]

Hierdie ontwikkelings weerspieël ’n breër verskuiwing: Openbare dienste, welsynsverspreiding, finansiële insluiting en selfs private kontrakte is nou gereeld afhanklik van biometriese-identifikasie- en digitale-verifikasie-platforms. Waar ’n identiteitsdokument of handmatige verifikasie in die verlede voldoende was, mag toegang tot maatskaplike toelaes, die bankwese, of selfs sekere nutsdienste nou biometriese verifikasie vereis. In werklikheid word inligtingsoorgawe ’n voorvereiste vir burgerlike deelname.

In hierdie konteks word toestemming as regverdiging vir die prosessering van persoonlike inligting diep problematies. Omdat datasubjekte realisties nie kan onttrek sonder om toegang tot noodsaaklike dienste prys te gee nie, stort die vrywilligheid wat ingevolge die Wet vereis word, inmekaar. Alhoewel die Wet op Beskerming van Persoonlike Inligting meer geskikte alternatiewe gronde vir regsgeldige prosessering bied (soos ’n regsverpligting of noodsaaklikheid vir die behoorlike uitvoering van ’n openbare regsplig), verdoesel die normatiewe en diskursiewe oorheersing van toestemming dikwels hierdie meer geskikte regverdiging in openbare-diens-kontekste.

https://doi.org/10.56273/1995-5928/2026/j23n2e5

Tesame demonstreer hierdie strukturele omstandighede – diep digitale ongelykheid en ongelyke digitale geletterdheid, wydverspreide platformafhanklikheid en die versnellende datafikasie van staats- en publieke-private infrastruktuur – hoe die kernelemente van toestemming onder die Wet op Beskerming van Persoonlike Inligting in die praktyk ondermyn word. Toestemming veronderstel vrywilligheid, ingeligte begrip, asook die vermoë om betekenisvol te kan weier. Tog is dit vir talle Suid-Afrikaners prakties onmoontlik om toestemming te weier (waar digitale platforms toegangspunte tot sosiale en ekonomiese deelname is), of regtens irrelevant (waar staatstelsels inligtingsoorgawe as ’n voorvereiste vir toegang tot noodsaaklike dienste vereis). Tschider voer aan dat toestemming dikwels as ’n vorm van risiko-aanvaarding funksioneer: Individue word geposisioneer asof hulle ingestem het om die gevolge van inligtingspraktyke, wat hulle nie kan onderhandel, verstaan of vermy nie, te aanvaar.[81] Hierdie dinamiek word versterk in struktureel ongelyke digitale omgewings waar beheer oor inligtingsinfrastrukture in magtige staats- en korporatiewe akteurs gekonsentreer is.

Hierdie realiteite beklemtoon ’n sentrale argument van hierdie artikel: Inligtingsbeskermingsreg kan nie verstaan of toegepas word in abstraksie van die sosiotegniese omstandighede waarin dit funksioneer nie. In die Suid-Afrikaanse konteks kan toestemming nie betroubaar as ’n primêre waarborg dien nie. ’n Reguleringsmodel wat gegrond is op formele opvattings van outonomie moet heroorweeg word in die lig van die strukturele beperkings wat mense se werklike keuses vorm.

5. Herbesinning van inligtingsbeskerming bo en behalwe toestemming

Die ontleding hier bo bewys dat die Wet op Beskerming van Persoonlike Inligting se afhanklikheid van toestemming konseptueel kragtig, maar prakties broos is. Die Wet stel ’n regulatoriese omgewing voor waarin datasubjekte inligtingspraktyke kan verstaan, risiko’s kan evalueer en betekenisvol ’n outonome keuse kan uitdruk. Hierdie aanname word egter ondermyn deur goed gedokumenteerde kognitiewe en gedragsbeperkings wat bepaal hoe individue werklik met toestemmingsprosesse omgaan. Individue vertrou op heuristieke om komplekse digitale omgewings te navigeer en is onderworpe aan standaardvooroordeel- en keuseargitekture wat daartoe aanleiding gee dat toestemming geroetineer en outomaties word, eerder as beraadslagend en doelgerig. Hierdie kognitiewe beperkings werk saam met, en word versterk deur, die strukturele omgewing wat Suid-Afrika se digitale ekosisteem definieer. Diep digitale ongelykheid, ongelyke digitale geletterdheid, platformafhanklikheid en die staat se groeiende datafikasie van openbare dienste werk almal om die infrastruktuur waardeur persoonlike inligting geprosesseer word, te verdoesel. Hierdie toestande maak nie net toestemming moeiliker om uit te oefen nie, maar ondermyn die presiese voorwaardes wat geldige toestemming moontlik sou maak.

Toestemming word dikwels as die standaard regverdiging vir die prosessering van persoonlike inligting beskou, maar die praktiese rol daarvan het verskuif: van die beskerming van outonomie na die verskaffing van institusionele dekking vir ondeursigtige, grootskaalse stelsels wat individue nie kan ondersoek nie. Gevolglik vra die regulatoriese raamwerk herhaaldelik dat datasubjekte verantwoordelikheid dra vir keuses wat hulle struktureel nie kan uitoefen nie. Dit is binne hierdie gaping waar die probleem van aanspreeklikheid ontstaan.

https://doi.org/10.56273/1995-5928/2026/j23n2e5

Alhoewel die Wet op Beskerming van Persoonlike Inligting ’n omvattende stel organisatoriese pligte bevat wat gewortel is in die beginsels van verantwoordingspligtigheid,[82] veiligheids-voorsorgmaatreëls[83] en deelname deur datasubjekte,[84] hang die doeltreffendheid van hierdie meganismes af van sterk institusionele toesig en betekenisvolle deursigtigheid. In die praktyk word Suid-Afrika se inligtingsbestuurslandskap gekenmerk deur voortdurende aanspreeklikheidsgapings wat hierdie statutêre verpligtinge ondermyn. Die feit dat die Inligtingsreguleerder onderbefonds en oorlaai bly, gee aanleiding tot vertraagde ondersoeke, beperkte proaktiewe monitering en die langsame ontwikkeling van afdwingingsnorme.[85] Terselfdertyd funksioneer sowel openbare as private liggame binne komplekse en dikwels ondeursigtige inligtingsekosisteme waarin inligting deur verskeie partye, verskaffers en infrastrukture vloei met minimale eksterne sekuriteit. Vir gewone datasubjekte maak hierdie ondeursigtigheid dit byna onmoontlik om vas te stel hoe hul inligting gebruik of misbruik word, wat ex post-regte soos toegang tot inligting,[86] beswaar[87] en regstelling[88] grootliks simbolies maak.

Hierdie strukturele swakhede ondermyn direk die grondslag waarop toestemming veronderstel is om te funksioneer. Toestemming veronderstel dat datasubjekte ingeligte keuses en hul regte effektief kan uitoefen en op instellings kan staatmaak om regspligte na te kom wanneer dinge skeefloop.[89] Indien toesig egter swak is en datapraktyke verborge bly, plaas die reg die verantwoordelikheid op datasubjekte, terwyl dit min praktiese vermoë aan hulle bied om prosessering te monitor of te betwis. Die resultaat is ’n diepgaande onsamehangendheid tussen die Wet op Beskerming van Persoonlike Inligting se formele argitektuur en sy beleefde werklikheid: ’n regulatoriese omgewing waar toestemming meer as ’n regsfiksie, eerder as ’n substantiewe waarborg, funksioneer. Om toestemming deur hierdie lens te herevalueer beklemtoon die noodsaaklikheid om dit te herposisioneer as ’n sekondêre, of uitsonderlike, grondslag vir prosessering, gereserveer vir kontekste waarin datasubjekte werklik betekenisvolle keuses kan uitoefen.

As toestemming struktureel ongeskik is vir baie Suid-Afrikaanse kontekste, moet die swaartepunt in die Wet op Beskerming van Persoonlike Inligting verskuif na die gronde vir regmatige prosessering wat reeds beter weerspieël hoe persoonlike inligting gebruik word: prosessering wat nodig is vir die afsluiting of uitvoering van ’n kontrak, vir nakoming van ’n regsverpligting, om ’n regmatige belang van die datasubjek te beskerm, of om openbare funksies na te streef. Hierdie grondslae erken die feit dat inligting in noodsaaklike dienste, platforminfrastrukture en staatsisteme ingebed is.

Die versterking van alternatiewe regsgronde vereis egter ’n ooreenstemmende verbetering van die Wet se afdwingingsargitektuur. Sonder doeltreffende toesig kan verantwoordelike partye hierdie grondslae ruim interpreteer, wat die beginselgebaseerde etos van die Wet ondermyn. Die Wet op Beskerming van Persoonlike Inligting bevat reeds sterk aanspreeklikheidsmeganismes op papier. Die probleem is nie leerstellige afwesigheid nie, maar institusionele swakheid. Die Inligtingsreguleerder het herhaaldelik ernstige hulpbron- en kapasiteitsbeperkings uitgelig wat dit nie in staat stel om nakoming op groot skaal te monitor, betyds op skendings te reageer, of sistemiese ondersoeke te doen nie. ’n Bestuursmodel wat minder klem op toestemming plaas, moet dus fokus op die praktiese uitvoering van die Wet se bestaande meganismes sodat institusionele verantwoordelikheid, eerder as individuele toestemming, die ruggraat van inligtingsbeskerming word.

https://doi.org/10.56273/1995-5928/2026/j23n2e5

6. Gevolgtrekking

In hierdie artikel is daar aangevoer dat hoewel die Wet op Beskerming van Persoonlike Inligting se toestemmingsraamwerk leerstellig gegrond is op die grondwetlike waardes van outonomie, waardigheid en selfbeskikking, die praktiese werking daarvan beperk word deur sowel kognitiewe realiteite as strukturele omstandighede binne Suid-Afrika se digitale omgewing. Kognitiewe en gedragsbeperkings soos heuristieke en begrensde rasionaliteit, gekombineer met strukturele faktore soos digitale ongelykheid, platformafhanklikheid en uitbreidende stelsels van staats- en privaat datafikasie, ondermyn egter die voorwaardes wat nodig is vir toestemming om as 'n effektiewe meganisme te funksioneer om inligtingsprosessering te regverdig.

Die Wet op Beskerming van Persoonlike Inligting bevat reeds 'n ryker aanspreeklikheidsraamwerk, gegrond op beginsels soos regmatigheid, oogmerkspesifikasie, minimaliteit en veiligheidsvoorsorgmaatreëls, wat die primêre verantwoordelikheid op verantwoordelike partye plaas, eerder as op datasubjekte. Die sentrale uitdaging is nie die afwesigheid van regsmeganismes nie, maar hul beperkte praktiese effek by ontstentenis van kragtige institusionele handhawing. Die versterking van die kapasiteit van die Inligtingsreguleerder, asook van strukturele aanspreeklikheidsmeganismes, sal Suid-Afrika se inligtingsbeskermingsregime beter belyn met sy grondwetlike grondslag. Om toestemming te herposisioneer as 'n aanvullende waarborg, eerder as die primêre meganisme vir beskerming, bied 'n meer realistiese en geregtigheidsgeoriënteerde grondslag vir inligtingsbeskerming in die Suid-Afrikaanse digitale omgewing.

Bibliografie

Bauer, J.M., R. Bergstrøm en R. Foss-Madsen. 2021. Are you sure, you want a cookie? – The effects of choice architecture on users' decisions about sharing private online data. *Computers in Human Behavior*, 210:106729.

Benyera, E. 2021. *The Fourth Industrial Revolution and the recolonisation of Africa*. Oxton: Routledge.

Carolan, E. 2016. The continuing problems with online consent under the EU's emerging data protection principles. *Computer Law and Security Review*, 32(3):462–73.

Chaka, C. 2022. Digital marginalization, data marginalization, and algorithmic exclusions: a critical southern decolonial approach to datafication, algorithms, and digital citizenship from the Souths. *Journal of E-Learning and Knowledge Society*, 18(3):83–95.

Chinembiri, T. 2020. Despite reduction in mobile data tariffs, data still expensive in South Africa (Policy Brief No. 2). *Research ICT Africa*. https://researchictafrica.net/research/despite-reduction-in-mobile-data-tariffs-data-is-still-expensive-in-south-africa (23 Julie 2026 geraadpleeg).

https://doi.org/10.56273/1995-5928/2026/j23n2e5

Chitimira, H., K. Motlogeloa en P. Magau. 2023. A legal analysis of the regulation of information and communications technologies to promote digital inclusion for the poor and low-income earners in South Africa. *Perspectives of Law and Public Administration*, 12(4):563–74.

Cinnamon, J. 2019. Attack the data: Agency, power, and technopolitics in South African data activism. *Annals of the American Association of Geographers*, 110(3):623–39.

Coleman, D. 2019. Digital colonialism: The 21st century scramble for Africa through the extraction and control of user data and the limitations of data protection laws. *Michigan Journal of Race and Law*, 24(1):417–39.

Custers, B., S. Van der Hof, B. Schermer, S. Appleby-Arnold en N. Brockdorff. 2013. Informed consent in social media use – The gap between user expectations and EU personal data protection law. *SCRIPTed: Journal of Law, Technology and Society*, 10(3):435–57.

Datareportal. 2025. Digital 2026: South Africa. Datareportal. https://datareportal.com/reports/digital-2026-south-africa (23 Julie 2026 geraadpleeg).

De Carvalho, D.F., C.N. Nobre en H.T. Marques-Neto. 2022. Evaluating cognitive privacy heuristics that influence Facebook user data disclosure. *Journal of Internet Services and Applications*, 13(1):66–81.

De Freitas, M.V. 2025. *Digital sovereignty and data colonialism: Shaping a just digital order for the Global South*. Benguerir: Policy Center for the New South.

Desai, A. 2018. Cybercrime, cybersurveillance and state surveillance in South Africa. *Acta Criminologica: Southern African Journal of Criminology*, 31(3):149–60.

De Stadler, E., I.L. Hattingh, P. Esselaar en J. Boast. 2021. *Over-thinking the Protection of Personal Information Act*. Kaapstad: Juta & Kie.

Ditlhokwa, G. en V.E. Cann. 2024. Platform dependency in the big tech era: lessons from Australian Facebook blackout and Botswana implications. *Studies in Media and Communication*, 12(3):25–35.

Europese Databeskermingsraad. 2020. Guidelines 05/2020 on consent under Regulation 2016/679. *European Data Protection Board*. https://www.edpb.europa.eu/documents/guideline/guidelines-052020-on-consent-under-regulation-2016679_en (23 Julie 2026 geraadpleeg).

Europese Parlement en Raad. 1995. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281, 23/11/1995, ble. 31–50.

https://doi.org/10.56273/1995-5928/2026/j23n2e5

Farronato, C., A. Fradkin en T. Lin. 2025. Designing consent: choice architecture and consumer welfare in data sharing. *Proceedings of the 26th ACM Conference on Economics and Computation*. https://dl.acm.org/doi/10.1145/3736252.3742627 (23 Julie 2026 geraadpleeg).

Froomkin, M.A. 2019. Big data: destroyer of informed consent. *Yale Journal of Law and Technology*, 21(3):27–54.

Govender, D. 2019. POPI versus technology: Did you consent to your toothbrush spying on you? *Without Prejudice*, 19(11):26–7.

Gutwirth, S., R. Leenes en P. de Hert (reds.). 2013. *Reloading data protection*. Dordrecht: Springer.

Inligtingsreguleerder Suid-Afrika. 2025. Information Regulator Annual Performance Plan 2025/2026. *InfoRegulator*. https://inforegulator.org.za/wp-content/uploads/2025/08/2025-2026-Annual-Performance-Plan.pdf.

Kahneman, D., J.L. Knetsch en R.H. Thaler. 1991. Anomalies: the endowment effect, loss aversion, and status quo bias. *Journal of Economic Perspectives*, 5(1):193–206.

Korobkin, R. 2003. Bounded rationality, standard form contracts, and unconscionability. *University of Chicago Law Review*, 70(4):1203–96.

Masur, P.K. 2020. How online privacy literacy supports self-data protection and self-determination in the age of information. *Media and Communication*, 8(2):258–69.

Monteleone, S. 2015. Addressing the "failure" of informed consent in online data protection: Learning the lessons from behaviour-aware regulation. *Syracuse Journal of International Law and Commerce*, 43(1):69–120.

Musoni, M. 2021. Challenges to POPIA compliance and enforcement. PPM Attorneys. https://www.ppmattorneys.co.za/popia-compliance (23 Julie 2026 geraadpleeg).

Njotini, M.N. 2018. Preserving the integrity of medical-related information. How "informed" is consent? *Potchefstroom Electronic Law Journal*, 21(1):1–20.

Nothias, T. 2025. An intellectual history of digital colonialism. *Journal of Communication*, 75(5):385–97.

OESO (Organisasie vir Ekonomiese Samewerking en Ontwikkeling). 1981. OECD guidelines governing the protection of privacy and transborder flows of personal data. https://www.oecd.org/en/publications/2002/02/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_g1gh255f.html (23 Julie 2026 geraadpleeg).

Raad van Europa. 1981. Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108). https://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_otros_documentos_UE_Convention_for_the_Protection.pdf.

https://doi.org/10.56273/1995-5928/2026/j23n2e5

Rhoen, M. 2016. Beyond consent: Improving data protection through consumer protection law. *International Policy Review*, 5(1):1–16.

Roos, A. 2020. The European Union's General Data Protection Regulation (GDPR) and its implications for South African data privacy law: an evaluation of selected "Content Principles". *Comparative and International Law Journal of Southern Africa*, 53(3):1–37.

—. 2023. Data protection principles under the GDPR and the POPI Act: a comparison. *Journal for Contemporary Roman-Dutch Law*, 86(1):1–26.

SARHK (Suid-Afrikaanse Regshervormingskommissie). 2009. Project 124 on Privacy and Data Protection. https://www.justice.gov.za/salrc/reports/r_prj124_privacy%20and%20 data%20protection2009.pdf.

SASSA (Suid-Afrikaanse Maatskaplike Sekerheidsagentskap). 2025. SASSA to introduce biometric enrolment in September. https://sassa.gov.za/documents/uploads/SASSA_to_ Introduce_Biometric_Enrolment_in_September.pdf.

Schermer, B.W., B. Custers en S. van der Hof. 2014. The crisis of consent: how stronger legal protection may lead to weaker consent in data protection. *Ethics and Information Technology*, 16(2):171–82.

Schultz, H. en W. Freedman. 2024. Plugins and POPI: a critical discussion into the legal implications of social plugins and the protection of personal information. *Potchefstroom Electronic Law Journal*, 27(1):1–32.

Sent, E.M. 2018. Rationality and bounded rationality: You can't have one without the other. *The European Journal of the History of Economic Thought*, 25(6):1370–86.

Statistiek SA. 2025. General Household Survey 2024. Statssa. https://www.statssa.gov.za/ publications/P0318/P03182024.pdf.

Suid-Afrikaanse Regering. 2025. Home Affairs launches Operation New Broom and biometric verification to combat illegal immigration. South African Government Official Information and Services. https://www.gov.za/news/media-statements/home-affairs-launches-operation-new-broom-and-biometric-verification-combat (23 Julie 2026 geraadpleeg).

Thaldar, D., A. Edgcumbe en D.L. Donnelly. 2023. How to interpret core concepts in POPIA? Recommendations on the draft Code of Conduct for Research. *South African Journal of Science*, 119(7/8):1–4.

Tschider, C.A. 2021. Meaningful choice: a history of consent and alternatives to the consent myth. *North Carolina Journal of Law & Technology*, 22(4):617–80.

Van Ooijen, I. en H.U. Vrabec. 2019. Does the GDPR enhance consumer's control over personal data? An analysis from a behavioural perspective. *Journal of Consumer Policy*, 42(1):91–107.

https://doi.org/10.56273/1995-5928/2026/j23n2e5

Warner, R. en R. Sloan. 2013. Beyond notice and choice: privacy, norms, and consent. *Journal of High Technology Law*, 14:1–34.

Woldegiorgis, E.T. 2022. Mitigating the digital divide in the South African higher education system in the face of the COVID-19 pandemic. *Perspectives in Education*, 40(3):197–211.

Zanfir, G. 2013. Forgetting about consent. Why the focus should be on "suitable safeguards" in data protection law. In Gutwirth e.a. (reds.) 2013.

Eindnotas

[1] De Stadler, Hattingh, Esselaar en Boast (2021:65); Govender (2019:27); Njotini (2018:3); Schultz en Freedman (2024:25–6).

[2] Alhoewel *datasubjekte* in die Wet op die Beskerming van Persoonlike Inligting 2013 (WBPI) gedefinieer word om regspersone in te sluit, sal die fokus vir doeleindes van hierdie artikel op individuele natuurlike persone as datasubjekte wees.

[3] Chaka (2022:86–7); Chitimera, Motlogeloa en Magau (2023:568–70).

[4] Chaka (2022:85); Chitimera e.a. (2023:563).

[5] SASSA (2025).

[6] Desai (2018:156); Suid-Afrikaanse Regering (2025).

[7] Kaneel (2019:624); De Freitas (2025:3); Rhoen (2016:3–4).

[8] De Stadler e.a. (2021); Govender (2019:27); Njotini (2018:3); Roos (2020); Roos (2023); Thaldar, Edgcumbe en Donnelly (2023).

[9] Sien Froomkin (2019); Custers, Van der Hof, Schermer, Appleby-Arnold en Brockdorff (2013); Rhoen (2016); Monteleone (2015); Tschider (2021); Zanfir (2013).

[10] SARHK (2009).

[11] Artikel 14 lui: "Elkeen het die reg op privaatheid, waarby inbegrepe is die reg dat hul persoon of woning nie deursoek word nie; hul eiendom nie deursoek word nie; daar nie op hul besittings beslag gelê word nie; of daar nie op die privaatheid van hul kommunikasies inbreuk gemaak word nie." Die aanhef tot die Wet op Beskerming van Persoonlike Inligting erken ook dat die reg op privaatheid 'n reg insluit op "beskerming teen die onregmatige insameling, behoud, verspreiding en gebruik van persoonlike inligting". (SARHK 2009:16–26)

[12] "Preserving privacy fosters individual autonomy, dignity, self-determination, and ultimately promotes a more robust, participatory citizenry." (SARHK 2009:16 nota 2)

[13] SARHK (2009:32).

https://doi.org/10.56273/1995-5928/2026/j23n2e5

[14] SARHK (2009:32).

[15] SARHK (2009:32–3).

[16] Die begrip *inligtingselfbeskikking* is afgelei van die Duitse reg soos bespreek in *Population Census Decision*, uitspraak van 15 Desember 1983, 1 BvR 209/83, BVerfGE 65, 1. Hierdie begrip het sentraal geword tot die Europese begrip van dataprivaatheid, en het as sodanig ook ’n invloed gehad op die Suid-Afrikaanse toepassing van die begrip.

[17] SARHK (2009:27–8).

[18] SARHK (2009:296).

[19] SARHK (2009:303–7).

[20] SARHK (2009:35).

[21] SARHK (2009:45–6).

[22] “In protecting a person’s personal information consideration should, therefore, also be given to competing interests such as the administering of national social programmes, maintaining law and order, and protecting the rights, freedoms and interests of others, including the commercial interests of industry sectors such as banking, insurance, direct marketing, health care, pharmaceuticals and travel services. The task of balancing these opposing interests is a delicate one.” (SARHK 2009:vii)

[23] “Privacy is therefore an important trade issue, as information privacy concerns can create a barrier to international trade. Considering the international trends and expectations, information privacy or data legislation will ensure South Africa’s future participation in the information market, if it is regarded as providing ‘adequate’ information protection by international standards.” (SARHK 2009:vii, 65)

[24] Raad van Europa (1981).

[25] OESO (1981).

[26] Europese Parlement en Raad (1995).

[27] Roos (2020:4); Tschider (2021:657).

[28] Regulasie (EU) 2016/679 van die Europese Parlement en van die Raad (Algemene Regulasie oor Databeskerming).

[29] De Stadler e.a. (2021:48); Roos (2023:3–4); Roos (2020:4).

[30] Inleiding tot die Wet op Beskerming van Persoonlike Inligting (voortaan in hierdie eindnotas oral “WBPI”).

[31] Artikel 4(1) van die WBPI.

https://doi.org/10.56273/1995-5928/2026/j23n2e5

[32] Artikel 11(1) van die WBPI.

[33] De Stadler e.a. (2021:198); Roos (2023:8–9); Roos (2020:15–6).

[34] "The 'notice' is a presentation of terms. The 'choice' is an act signifying acceptance of the terms (typically using the site or clicking on an 'I agree' button)." (Warner en Sloan 2013:3)

[35] Artikel 1 van die WBPI.

[36] Artikel 2(h) van die Databeskermingsriglyn.

[37] Artikel 4(11) van die Algemene Regulasie oor Databeskerming.

[38] De Stadler e.a. (2021:66–9); Roos (2023:3–4); Roos (2020:14–5).

[39] De Stadler e.a. (2021:6); Roos (2020:16–7); Thaldar e.a. (2023:1).

[40] De Stadler e.a. (2021:67); Europese Databeskermingsraad (2020:7).

[41] De Stadler e.a. (2021:67); Europese Databeskermingsraad (2020:10–1).

[42] Artikel 13(1) van die WBPI bepaal: "Persoonlike inligting moet vir 'n bepaalde, uitdruklik omskrewe en regmatige oogmerk wat verband hou met 'n werksaamheid of aktiwiteit van die verantwoordelike party ingesamel word."

[43] De Stadler e.a. (2021:67); Europese Databeskermingsraad (2020:12); Roos (2020:15).

[44] Europese Databeskermingsraad (2020:14).

[45] De Stadler e.a. (2021:68).

[46] Artikel 18(1) van die WBPI.

[47] De Stadler e.a. (2021:68).

[48] Artikel 22(1) van die Verbruikersbeskermingswet 68 van 2008.

[49] Artikel 22(2) van die Verbruikersbeskermingswet.

[50] De Stadler e.a. (2021:69); Europese Databeskermingsraad (2020:18); Roos (2020:15).

[51] De Stadler e.a. (2021:69); Europese Databeskermingsraad (2020:18–19); Roos (2020:15).

[52] Artikel 69(1)–(2) van die WBPI. Die Inligtingsreguleerder het 'n vorm uitgereik (Vorm 4) wat die vorm voorskryf waarin toestemming onder hierdie omstandighede verkry moet word. (Vorm 4 van die Regulasies rakende die Beskerming van Persoonlike Inligting, 2018.)

[53] Rhoen (2016:5–6); Tschider (2021:659).

https://doi.org/10.56273/1995-5928/2026/j23n2e5

[54] Dit beteken dat mense ’n heuristiese benadering tot besluitneming gebruik, wat gekenmerk word as nie ten volle geoptimaliseer, perfek of gerasionaliseer nie, maar tog “goed genoeg”. Hierdie kognitiewe kortpaaie lei dikwels tot vooroordele en slegte besluite. Sien Korobkin (2003); Sent (2018).

[55] Korobkin (2003:1222–5); Sent (2018:1374).

[56] Artikel 18 van die WBPI.

[57] Schermer, Custers en Van der Hof (2014:176–7). Sien ook De Carvalho, Nobre en Marques-Neto (2022).

[58] De Carvalho e.a. (2022); Van Ooijen en Vrabec (2019:94–6).

[59] Schermer e.a. (2014:177); Carolan (2016:470–1).

[60] Schermer e.a. (2014:176); Monteleone (2015:88); Van Ooijen en Vrabec (2019:95).

[61] Monteleone (2015:89–90); De Carvalho e.a. (2022); Schermer e.a. (2014:176–8).

[62] Kahneman, Knetsch en Thaler (1991:198–9); Korobkin (2003:1229–34); Rhoen (2016:3–4).

[63] Bauer, Bergstrøm en Foss-Madsen (2021:1–2); sien ook Farronato, Fradkin en Lin (2025).

[64] Monteleone (2015:89–90); Carolan (2016:470–1); Bauer e.a. (2021:5); Froomkin (2019:31).

[65] Warner en Sloan (2013:2); Monteleone (2015:73–4); Rhoen (2016:2); Tschider (2021:658); Zanfir (2013:242).

[66] Datareportal (2025); Statistiek SA (2025:51).

[67] Statistiek SA (2025:51).

[68] Datareportal (2025); Statistiek SA (2025:51).

[69] Chinembiri (2020); Datareportal (2025); Statistiek SA (2025:53).

[70] Chaka (2022:87); Chitimira e.a. (2023:569); Woldegiorgis (2022:200–1).

[71] Chaka (2022:85); Chitimira e.a. (2023:572–3); Ditlhokwa en Cann (2024:28).

[72] Chitimira e.a. (2023:563).

[73] Datareportal (2025).

[74] Ditlhokwa en Cann (2024:31).

[75] Chaka (2022:85–7); Chitimera e.a. (2023:563–64); Woldegiorgis (2022:202).

https://doi.org/10.56273/1995-5928/2026/j23n2e5

[76] Custers e.a. (2013:452–3); Masur (2020:266); Monteleone (2015:83–4).

[77] Benyera (2021:1–16); Custers e.a. (2013:452–3); Rhoen (2016:3–4).

[78] Chaka (2022:84); Coleman (2019:422–3); De Freitas (2025:3–4); Nothias (2025:386–9); Benyera (2021:1–16).

[79] SASSA (2025).

[80] Suid-Afrikaanse Regering (2025).

[81] Tschider (2021:652).

[82] Artikel 8 van die WBPI.

[83] Artikels 19–22 van die WBPI.

[84] Artikels 23–25 van die WBPI.

[85] Inligtingsreguleerder Suid-Afrika (2025:25–6); Musoni (2021).

[86] Artikel 23 van die WBPI.

[87] Artikels 5(*e*), 11(3)(*a*), 69(3), 28(1)(*c*), 32(1)(*b*)(i) en 70(2) van die WBPI.

[88] Artikel 24 van die WBPI.

[89] Custers e.a. (2013:444–9); Monteleone (2015:83–6); Rhoen (2016:4–6).