’n Toepaslike regsraamwerk vir geoutomatiseerde gesigherkenningstegnologie in Suid-Afrika

Barrie J. Gordon

Barrie J. Gordon, Departement Straf- en Prosesreg, Universiteit van Suid-Afrika

Opsomming

Geoutomatiseerde gesigherkenning (GGH) is ’n nuwe tegnologie wat rekenaars in staat stel om mense te identifiseer sonder dat ’n operateur betrokke hoef te wees. Dit verskaf ’n legio aanwendings in die privaat- en openbare sektore, en kan ook baie nuttig in wetstoepassingsituasies gebruik word. Aangesien GGH-stelsels vinnig en wydverspreid aangewend kan word, hou hierdie tegnologie egter ook die gevaar in dat dit op grootskaalse wyse tot menseregteskendings aanleiding kan gee. Dit is daarom van kritieke belang dat daar ’n betekenisvolle balans verkry moet word tussen die gebruik van GGH-stelsels en die beskerming van menseregte.

Die onlangse Britse beslissing in *The Queen (on application of Edward Bridges) v The Chief Constable of South Wales Police* (2020) EWCA Civ. 1058 toon aan hoe so ’n balans moet lyk. Die kernaangeleentheid is dat daar ’n toepaslike regsraamwerk geskep moet word waarbinne enige GGH-stelsel behoort te funksioneer. Dit behels dat die magtigende wetgewing so geformuleer moet word dat dit individuele diskresie van wetstoepassers beperk, en ook meganismes daarstel waar menslike operateurs steeds die finale besluite oor GGH moet neem.

Daar bestaan reeds ’n basiese raamwerk vir die ontplooiing van GGH-stelsels in Suid-Afrika in die vorm van die Grondwet van die Republiek van Suid-Afrika van 1996, die Wet op Beskerming van Persoonlike Inligting 4 van 2013, en die Wetsontwerp op Kubermisdade van 2017. Deur die gebruik van verskeie meganismes in hierdie wetgewing kan die toepaslike regsraamwerk verder uitgebou word om GGH-stelsels veilig in Suid-Afrika te ontplooi.

Trefwoorde: biometriese inligting; *Bridges*; geoutomatiseerde gesigherkenning (GGH); geoutomatiseerde gesigherkenningstegnologie; gesigbiometrika; menseregte; POPI; regsraamwerk; regulering; Vumacam; Wet op Beskerming van Persoonlike Inligting; wetstoepassing

Abstract

An appropriate legal framework for automated facial recognition in South Africa

Automated facial recognition (AFR) is a new technology that enables computers to individualise people without the input of a human operator. It has a myriad of applications in the private and public sectors and can be used by law enforcement to identify suspects in large groups. However, AFR also has the potential for enormous human rights abuses. People's movements can be determined, and if linked to pre-existing systems, such as a state's driver's license database, it is possible to monitor the movements of total populations. As a result, it is of the utmost importance that the use of such systems should remain within the legal sphere, and that legal principles governing such systems are clear and well defined. It is important that individuals' discretion in the use of such systems is limited to prevent abuse of power.

AFR technology simply determines whether two photos are those of the same person. The system takes a picture of a known person and creates a simple triangulated map by connecting general details of the face and measuring those lines. For example, the technology can determine how wide the eyes and nose are, where the lines of the mouth and eyebrows run, and the shape of the face and ears. These points are then linked together, their lengths are measured, and the dimensions and identity of the person are stored as a simple list of digits, in a certain order, in a database. When these simple facial details are linked with a larger system, the system becomes so powerful that it is possible to identify people. In such a system a second video source is necessary, for example where a group of people passes in front of a closed-circuit television (CCTV) camera. The system will process the facial biometrics of all the people in the video, feed them into and compare them with the original database where the identity of individuals is known. If the AFR system makes a positive match, the system operator learns the person's identity.

The legality of AFR technology was recently decided in the United Kingdom (UK) in *The Queen (on application of Edward Bridges) v The Chief Constable of South Wales Police* (2020) EWCA Civ. 1058 (*R-Bridges*), the first case of its kind in the world. The court confirmed that the core issue of this matter is whether an appropriate legal framework exists within which AFR can be legally deployed. Several pieces of legislation were scrutinised to determine whether AFR functions within the law. The first of these is article 8 of the European Convention on Human Rights, which regulates the right to privacy. In *PG v United Kingdom* (2008) 46 EHRR 51, 57 the court ruled that article 8 could be violated if new technology was used in such a way that it preserves a permanent record of public events. The Court of Appeal confirmed this statement in *R-Bridges*. Secondly, the Surveillance Camera Code of Practice, enacted under section 29 of the Protection of Freedoms Act 2012, seeks to protect human rights by establishing guidelines that restrict camera operators' discretion when working with CCTV video footage. It also regulates the storage of and access to data. Thirdly, various sections of the Data Protection Act 2018 regulate the collection of data, as well as its storage. These legislative measures contain the enabling legislation within which AFR should operate in the UK. It was decided in *R-Bridges* that the defendant had gone beyond legislative provisions when deploying AFR, and issued a declaratory statement to resolve the matter between the parties.

As in the UK, several legislative tools in South Africa contain the enabling legislation for AFR. The Protection of Personal Information Act 4 of 2013 (POPI) is the first of these, and regulates

the collection, storage and further processing of personal information. Several sections are applicable to AFR, and anyone wanting to implement an AFR system in South Africa will have to take note of all relevant provisions in this act. The POPI Act stipulates that the Regulator may issue codes of conduct which will be applicable to specific situations. It is therefore possible to write a code of conduct which specifically sets out the principles applicable to AFR. This would be akin to the UK Surveillance Camera Code of Practice, and such a code could make a meaningful contribution to the law, provided it is formulated correctly. Section 45 of the Cybercrime Bill of 2017 regulates the possession of data by police officials. In the context of AFR, police officials can obtain CCTV video footage from third-party service providers simply by getting their permission to view the material. If the service provider is willing to provide specific information, like street-camera footage, to law enforcement officials, it can be lawfully obtained and viewed by them. This provides too much discretion to individual parties, and could easily be an abuse of human rights.

The unreported judgment of *Vumacam v Johannesburg Road Agency* 2020-08-20 case no. 14867/20 (HHSA) illustrates the atmosphere and views when sensitive biometric information is involved. In this case the Johannesburg Roads Agency (JRA) refused to issue wayleaves to Vumacam, because it believed that Vumacam had abused their power by spying on innocent people and selling the "footage" to third parties. JRA further felt that Vumacam's "spy footage" was a tradable asset in their hands, and that this was the primary reason for installing the cameras. In essence the JRA accused Vumacam of spying on individuals' movements and thereby infringing on their right to privacy. It is very interesting that the JRA, like the Court of Appeal in *R-Bridges*, argued that a legal framework must be in place before such sensitive biometric data can be collected and processed and that it should respect individuals' privacy rights. Vumacam retaliated by explaining that the cameras had been installed for crime prevention purposes. It further claimed that the JRA was in no position to deny wayleave applications, as Vumacam complied with the requirements as contained in the legislation.

To reach a correct finding, the court examined the local legislation applicable to this case and concluded that if it appears that the service provider has been approved to work around public roads, and it appears that the necessary procedures are in place to protect the infrastructure, the authorising authority must grant the application. Nowhere in the legislation is any mention made of a provision that the authorising authority (in this case the JRA) may refuse an application on any other grounds not contained in the legislation. Consequently, the case was decided in favour of Vumacam. It should be stated clearly that Vumacam's victory had nothing to do with the issue of potential privacy breaches. At the heart of the matter was the JRA's refusal for considering Vumacam's applications for wayleaves. In that regard the JRA erred in considering factors other than those outlined in the empowering legislation. The importance of the case is that it illustrates the general legal sense regarding AFR and the processing of sensitive biometric data. One of the critically important requirements for the successful implementation of AFR without committing large-scale human rights violations is a comprehensive legal framework that restricts individual discretion and prohibits unnecessary processing of sensitive data. Currently Vumacam is at liberty to record and store CCTV footage at will, without any specific legislation regulating how this material should be handled and stored.

Several recommendations may be made. The first is that the exceptions in the POPI Act are too broad for providing meaningful human rights protection. The South African legal framework gives too much discretion to individual operators, which increases the possibility of human

rights violations. Secondly, it appears that ordinary CCTV footage can be used as a data source for AFR systems. The UK Surveillance Camera Code of Practice contains comprehensive regulations for CCTV operators. No similar regulations are in place in South Africa, and as a result it is not surprising that the JRA is so concerned about Vumacam's wide discretion regarding CCTV technology. The POPI Act allows for the creation of codes of conduct, and these provisions should be used to create codes regulating CCTV and AFR use. It is strongly recommended that codes of such nature be issued in South Africa as a matter of urgency. Thirdly, it seems that with any AFR system a human should be the final decision maker. This is something the *Bridges* ruling emphasised, and fortunately it is also something that is pertinently addressed in the POPI Act. South Africa has the fragments of a legal framework to implement AFR successfully. Just as with our UK counterpart, the law should be developed and expanded to safeguard human rights in an era where new technology has the potential to infringe on human domains like never before.

Keywords: automated facial recognition (AFR); automated facial recognition technology; biometric information; *Bridges*, facial biometrics; human rights; law enforcement; legal framework; Protection of Personal Information Act (POPI Act); regulation; Vumacam

1. Inleiding

Geoutomatiseerde gesigherkenning (GGH) is 'n nuwe tegnologie wat rekenaars in staat stel om persone te individualiseer sonder dat die insette van 'n menslike operateur nodig is.[1] Op Engels staan dit bekend as Automated Facial Recognition (AFR).[2] Hierdie tegnologie het 'n magdom toepassingsgebiede in die privaat- en openbare sektore, en kan met vrug deur wetstoepassers ingespan word om verdagtes in groot groepe te identifiseer.[3] GGH het egter ook die potensiaal tot enorme menseregtevergrype.[4] Mense se bewegings kan bepaal word, en indien dit met reeds bestaande stelsels, soos 'n staat se rybewysdatabasis, gekoppel word, is dit moontlik om totale bevolkings se bewegings te monitor.[5] Dit is daarom van die uiterste belang dat die gebruik van sulke stelsels binne die regsfeer bly en dat die regsbeginsels wat die stelsels reguleer, duidelik en goedgedefinieer is. Dit is belangrik dat individue se diskresie in die gebruik van die stelsels beperk sal word sodat magsvergrype nie maklik kan geskied nie.[6]

Die doel van hierdie bydrae is om die regsraamwerk van GGH in Suid-Afrika te skets. Dit poog om in breë trekke te bepaal watter Suid-Afrikaanse wetgewing op GGH van toepassing sal wees wanneer dit hier in werking gestel word.

Twee Britse hofbeslissings het onlangs GGH in wetstoepassing ondersoek. Die eerste is *Edward Bridges v The Chief Constable of South Wales Police*[7] *(Bridges)*, en die tweede is dieselfde saak wat in appèl geneem is, naamlik *The Queen (on application of Edward Bridges) v The Chief Constable of South Wales Police*[8] *(R-Bridges)*. Uit hierdie sake blyk duidelik dat dit krities belangrik is om te bepaal watter regsbeginsels op GGH van toepassing is, of dit voldoende is, en waar uitbreidings nodig is.[9]

Hierdie bydrae gaan 'n soortgelyke struktuur volg. In die eerste plek sal 'n oorsig oor GGH-tegnologie gegee word sodat die regskwessies beter begryp kan word. Dan sal die regsraamwerk wat in Brittanje geld, soos deur die *Bridges*-beslissings toegelig is, onder die loep geneem word.[10] Soortgelyke wetgewing in Suid-Afrika sal vervolgens bespreek word

waar daar bepaal kan word in watter mate dit op GGH van toepassing is. Ter afsluiting sal aanbevelings gemaak word oor waar Suid-Afrikaanse wetgewing te kort skiet, en hoe dit verbeter kan word.

2. Die tegnologie

GGH is 'n nuwe tegnologie wat eenvoudig bepaal of twee foto's dié van dieselfde persoon is.[11] Die stelsel neem 'n foto van 'n persoon as basis en skep 'n eenvoudige driehoekkaart deur algemene besonderhede van die gesig met mekaar te verbind en daardie lyne te meet.[12] Daar word byvoorbeeld bepaal hoe breed die oë en neus is, waar die lyne van die mond en oogbanke loop, en wat die vorm van die gesig en ore is. Hierdie punte word dan met mekaar verbind, die lengte daarvan word gemeet, en die afmetings word as 'n eenvoudige lys van syfers, in 'n sekere volgorde, in 'n databasis gestoor.[13] Wanneer dié eenvoudige gesigbesonderhede in 'n groter stelsel geplaas word, word dit so kragtig dat dit moontlik is om individuele persone te identifiseer.[14] Die manier waarop dit gedoen word, is dat foto's van persone wie se identiteit reeds bekend is, aan 'n GGH-stelsel blootgestel word. Die stelsel verwerk dan die persoon se gesigbesonderhede soos hier bo verduidelik, en berg dit in 'n databasis saam met die persoon se identiteit. Hierdie databasis vorm dan die bron waarmee nuwe inligting vergelyk kan word.[15]

Om egter enige sinvolle inligting uit die stelsel te verkry, is 'n tweede voedingsbron nodig. Dit word gewoonlik verkry van beeldmateriaal van geslotebaantelevisie[16] (CCTV), waar die stelsel 'n groep mense wat voor die kamera verby beweeg, individualiseer deur elke persoon in sy eie foto te plaas.[17] Dan word dieselfde driehoekkaart van die gesig geskep, dit word gemeet, en die besonderhede word met dié in die brondatabasis van bekende persone vergelyk. Indien daar 'n positiewe verwantskap is, word die identiteit van die persoon in die CCTV-beeldmateriaal aan die stelseloperateur bekend.[18] Uit hierdie inligting is dit duidelik dat die stelseloperateur nooit die identiteite van die legio mense in die CCTV-beeldmateriaal kan bepaal as daar nie 'n databasis bestaan waarteen die biometriese inligting vergelyk kan word nie.[19] Dus, ten spyte daarvan dat gesigbiometrika in die CCTV-beeldmateriaal verwerk word, bly die identiteit van die persoon onbekend totdat daardie persoon se identiteit vanuit die brondatabasis geopenbaar word.[20] Dit gebeur natuurlik slegs as daar 'n verwantskap tussen die item van die brondatabasis en voedingsdata bestaan.[21]

3. Geoutomatiseerde gesigherkenningstegnologie in die Verenigde Koninkryk

3.1 Bridges-beslissings

In 2017 het die Suid-Wallis Polisiedepartement begin eksperimenteer met die gebruik van GGH in wetstoepassing.[22] Die eiser, Edward Bridges, was by twee geleenthede binne die trefwydte van hierdie stelsels.[23] As burgerregtekampvegter het Bridges besluit om die Suid-Wallis Polisiedepartement voor die hof te daag, aangesien hy van mening was dat die gebruik van GGH in hierdie gevalle nie wettig is nie.[24] Die saak het eers voor die plaaslike afdeling van die Cardiff Hoë Hof gedien, waar die eis van die hand gewys is.[25] Hierna het Bridges die saak in appèl na Londen geneem, waar verskeie van sy eise toegestaan is.[26]

Aangesien dit die eerste hofsaak in die wêreld is wat spesifiek GGH bespreek, het die hof van appèl spesiale moeite gedoen om die kwessies ter sprake so noukeurig as moontlik na te gaan.[27] Uit beide hofuitsprake blyk dat die kernaangeleentheid is of daar 'n toepaslike regsraamwerk bestaan waarbinne GGH regtens ontplooi kan word.[28] Met ander woorde, mag die Suid-Wallis Polisiedepartement enigsins GGH toepas indien daar nie spesifiek wetgewing bestaan wat dit reguleer nie? Beide howe het dit duidelik gemaak dat ten spyte daarvan dat GGH 'n nuwe tegnologie is, dit wetstoepassers nie verhinder om dit te gebruik nie.[29] Genetiese DNS-toetsing en vingerafdrukke was ook op 'n stadium nuwe tegnologieë, maar solank daar algemene wetgewing bestaan waarbinne hierdie nuwe tegnologieë kan funksioneer, mag dit gebruik word.[30] Wat egter in hierdie konteks van belang is, is om te bepaal wat die magtigende wetgewing behels, of dit voldoende is, en of die Suid-Wallis Polisiedepartement binne die sfeer van die reg gebly het.

Hierdie bydrae gaan nie poog om die twee *Bridges*-sake in besonderhede te bespreek nie. Wat hier ter sprake is, is eerder die afbakening van die toepaslike regsraamwerk waarbinne GGH kan funksioneer. Wanneer dit gedoen is, kan die regsraamwerk met dié van Suid-Afrika vergelyk word om te bepaal of ons regstelsel voldoende ontwikkel is om die publiek se regte in 'n GGH-ontplooiing te beskerm.

In die *Bridges*-beslissings is verskeie Britse wette en 'n internasionale konvensie geïdentifiseer wat op GGH van toepassing is, en dit word vervolgens bespreek om die regslandskap waarbinne GGH behoort te funksioneer, af te baken.

3.2 Europese Konvensie vir Menseregte

Die Europese Konvensie vir Menseregte, wat reeds in 1950 die lig gesien het, bevat onder andere 'n handves van menseregte.[31] Artikel 8(1) bepaal dat elkeen die reg op respek vir sy privaat- en gesinslewe het, terwyl subartikel (2) noem dat 'n publieke owerheid nie op hierdie reg mag inmeng nie, mits dit "in accordance with the law" is. Etlike hofuitsprake het al beslis dat hierdie bepaling nie beperk is tot 'n persoon se private sfeer nie, maar dat dit ook in die openbaar van toepassing is.[32] Indien 'n persoon se optrede op een of ander manier vasgelê word, sodat daar 'n rekord daarvan bestaan, kan dit binne die sfeer van menseregteskendings val. In *PG v United Kingdom* (2008) 46 EHRR 51 op 57 word dit só gestel:

> A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private-life considerations may arise, however, *once any systematic or permanent record comes into existence of such material from the public domain* …[33]

Wanneer hierdie uitspraak in ag geneem word, is dit baie duidelik dat artikel 8 van die Europese Konvensie vir Menseregte geskend kan word indien GGH só ingespan word dat 'n permanente rekord van die publieke gebeure geberg word. Dit is dan ook presies wat die hof van appèl in *R-Bridges* beslis het.[34]

3.3 Protection of Freedoms Act 2012

Daar is reeds hier bo aangetoon dat GGH die videomateriaal van 'n gewone CCTV-kamera as invoerdata kan gebruik.[35] Daarom is dit nie vreemd dat Britse wetgewing wat oor CCTV-

kameras handel, ook op GGH van toepassing kan wees nie. Artikel 29 van die Protection of Freedoms Act 2012 meld dat die staatsekretaris 'n praktykskode vir CCTV-kameras moet ontwikkel wat spesifiek aandui watter beginsels toegepas moet word wanneer 'n CCTV-kamera in die openbaar ontplooi word.[36] Daar word ook bepaal dat dit gereeld bygewerk moet word om die nuutste, beste gebruike in die bedryf te verteenwoordig.[37]

Die resultaat van hierdie wetgewing is die baie insiggewende Surveillance Camera Code of Practice.[38] In paragraaf 2.6 daarvan word 12 riglyne neergelê waaraan alle operateurs van CCTV-kameras moet voldoen.[39] Wanneer die riglyne gelees word, is dit duidelik dat baie navorsing gedoen is om die riglyne so te skryf dat dit die beste vorm van menseregte-beskerming bied terwyl dit die grootste mate van vryheid aan operateurs verskaf. Uit die aard van sy werking sal 'n waarnemingskamera[40] altyd op een of ander manier op mense se vryhede inbreuk maak. Die 12 riglyne bepaal kortliks dat wanneer so 'n kamera gebruik word, dit gedoen behoort te word slegs om 'n spesifieke doel te dien.[41] Wanneer dit ontplooi word, moet die publiek se reg op privaatheid voor oë gehou word, en moet dit ook deursigtig vir die publiek wees.[42] Operateurs van waarnemingskameras moet verantwoordelik gehou word vir die gebruik van die kameras, en dit beteken dat duidelike reëls en regulasies moet bestaan om individuele diskresie te beperk.[43] Wanneer waarnemingskameras se beeldmateriaal gestoor word, is dit van die uiterste belang dat slegs die minimum hoeveelheid inligting behou word, en niks meer nie.[44] Toegang tot gestoorde beeldmateriaal moet beperk word, en daar moet sekuriteitsmaatreëls in plek wees om sulke beperkte toegang te beheer.[45] Om te verseker dat daar aan al hierdie vereistes voldoen word, moet daar 'n ouditsisteem bestaan om potensiële individuele magsvergrype uit te skakel.[46]

Wanneer hierdie riglyne ondersoek word, blyk dit dat die reguleerder[47] se fokus drieledig is: Eerstens word riglyne neergelê om die kamera-operateur se diskresie te beperk; tweedens word die publiek se menseregte voor oë gehou; en derdens word streng maatreëls daargestel om die berging van en toegang tot data te beperk. Dit is dus die basiese beginsels waaraan enige regsraamwerk moet voldoen om sinvolle menseregtebeskerming te verseker.

3.4 Data Protection Act 2018

Artikels 35, 42 en 64(1) van die Data Protection Act 2018 bevat die relevante inligting wat op GGH van toepassing is. In die eerste plek sit artikel 35 die beginsels uiteen waaraan voldoen moet word voordat sensitiewe data ingewin en verwerk mag word. Dit bepaal dat alle verwerking van persoonlike inligting wettig en regverdig moet wees;[48] dat die *data subject* toestemming moet gee tot die verwerking van die inligting, of dat die insameling daarvan nodig is om die wetstoepasser se doel daarmee te bereik,[49] en dat 'n toepaslike beleidsdokument moet bestaan indien sensitiewe data verwerk word.[50] In die tweede plek word biometriese data as sensitiewe data beskou,[51] en daarom sal 'n wetstoepasser in Brittanje 'n beleidsdokument moet daarstel alvorens enige pogings om GGH te implementeer, uitgevoer word. Artikel 42 verduidelik in besonderhede watter vereistes vir sensitiewe data gestel word. In wese beteken dit dat die beleidsdokument die prosedures wat gevolg gaan word, uiteen moet sit[52] en wanneer sensitiewe data geberg gaan word, moet daar aangedui word hoe lank die data gehou gaan word, en watter prosedures gebruik sal word wanneer dit uitgewis word.[53] Derdens bepaal artikel 64 bloot dat wanneer daar 'n groot risiko bestaan dat daar op individue se regte inbreuk gemaak gaan word, 'n impakstudie vooraf gedoen moet word.[54]

Hierdie drie bepalings het maar eintlik dieselfde doel voor oë as wat hier bo by die Surveillance Camera Code of Practice bespreek is: Dit gaan oor die beskerming van menseregte, terwyl daar aanvaar word dat wetstoepassers daarop inbreuk kan maak, maar dat wanneer dit gebeur, die invloed daarvan beperk moet word. Die doel van die beleidsdokumente en impakstudie is dan ook om ’n vorm van oudit in die stelsel in te bou sodat latere beoordelaars, soos polisiehoofde of howe, kan oordeel of daar wettig opgetree is.

3.5 Equality Act 2010

Artikel 149 van die Equality Act 2010 bepaal dat ’n openbare owerheid altyd moet poog om enige vorm van diskriminasie op grond van onder andere ras en geslag uit te skakel.[55] Hierdie strewe word uitgedruk as ’n *Public Sector Equality Duty*, en is iets wat baie ernstig in Brittanje opgeneem word.[56] In beide die *Bridges*-beslissings is daar verduidelik hoe dit moontlik is dat ’n GGH-stelsel bevooroordeeld ten opsigte van ras en geslag kan wees.[57] Kundige getuies het aan die hof verduidelik dat die GGH-algoritmes met sekere databasisse opgestel word, en indien ’n databasis van ’n spesifieke etniese groep, soos “white North European”[58] persone, gebruik word, dit meer vals positiewe resultate ten opsigte van ander etniese groepe asook vrouens sal vertoon.[59] Selfs al word die algoritme op ’n verskeidenheid databasisse van verskillende etniese oorsprong opgestel, is daar steeds anomalieë, aangesien die databasisse van Europese oorsprong meer ontwikkeld as dié van ander etniese groepe is. Gevolglik is dit moontlik dat die sagteware meer vals positiewe resultate ten aansien van persone soos Asiërs, Afrikane[60] en vroue lewer.[61]

In die konteks van GGH is dit belangrik om die werking van die spesifieke sagteware wat vir wetstoepassing gebruik word, te toets en die resultate goed te verstaan.[62] Verskillende verskaffers se GGH-algoritmes lewer verskillende resultate, en wetstoepassers moet bewus wees van die sagteware se tekortkomings. Dit is egter iets wat dikwels moeilik is om vooraf te bepaal, aangesien GGH-verskaffers nie graag inligting oor die databasisse wat hul gebruik om die algoritmes op te stel, openbaar wil maak nie. Die veld van GGH-sagteware is baie mededingend, en die openbaarmaking van sulke inligting kan die verskaffer se mededingende voordeel benadeel.

3.6 Gevolgtrekking

Brittanje het verskeie stukke wetgewing wat op GGH toegepas kan word. Aan die een kant bestaan daar wetgewing soos die Europese Konvensie vir Menseregte wat menseregte identifiseer en uiteensit. Aan die ander kant bestaan daar verskeie wette wat die inwin en verwerking van sensitiewe data, soos biometrika, reguleer. Tegnologieë soos CCTV word pertinent aangespreek, en daar word pogings aangewend om rasse-ongelykheid uit die weg te ruim. Dit is daarom nie vreemd dat die hof in *R-Bridges* beslis het dat Brittanje inderdaad oor ’n regsraamwerk beskik om GGH te reguleer nie. Dat hierdie regsraamwerk steeds te kort skiet, is seker, maar dat algemene wetgewing op GGH toegepas kan word, staan ewe vas. Die *Bridges*-sake was in ’n sekere sin ’n oorwinning vir beide partye. Bridges het enersyds die bevrediging gekry om te weet dat die hof van appèl beslis het dat die Suid-Wallis-polisie nie hul wetlike verpligtinge nagekom het nie.[63] Andersyds het die Suid-Wallis-polisie en die Britse wetgewer uitgevind waar hul beleide en wetgewing te kort skiet.[64]

Vervolgens word ’n soortgelyke regsraamwerk in Suid-Afrika ondersoek, en deur dit met die raamwerk wat hier bo bespreek is te vergelyk, kan bepaal word of daar voldoende voorsiening gemaak word in ons reg vir wanneer GGH hier ingespan gaan word.

4. Geoutomatiseerde gesigherkenningstegnologie (GGH) in Suid-Afrika

4.1 Biometrika

Die Suid-Afrikaanse wetgewer het nog nie spesifieke wetgewing aanvaar wat GGH hanteer nie. Tog is dit ’n kenmerk van die reg dat algemene beginsels dikwels op nuwe situasies toegepas kan word. Indien GGH gekategoriseer moet word, is dit duidelik dat dit binne die groter veld van biometrika val. Die Suid-Afrikaanse wetgewer het reeds by verskeie geleenthede die kwessie van biometriese inligting onder die loep geneem. Die Wet op die Registrasie van Geboortes en Sterftes 51 van 1992 definieer *biometrika* as “foto’s, vingerafdrukke (insluitend palmafdrukke), handafmetings, handtekeningverifikasie of retinapatrone wat gebruik kan word om die identiteit van individue te verifieer”.[65] Dit is baie duidelik dat hierdie definisie te beperkend vir GGH is en dit nie voldoende aanspreek nie. Die wetgewer se definisie van *biometrika* in die Wet op Beskerming van Persoonlike Inligting 4 van 2013 is heelwat beter. Dit word beskryf as “’n tegniek van persoonlike identifikasie wat gebaseer is op fisiese, fisiologiese of gedragskarakterisering, met inbegrip van bloedgroepering, die neem van vingerafdrukke, DNS-ontleding, retinale skandering en stemherkenning”. Ook hierdie definisie maak nie spesifiek voorsiening vir GGH nie, maar die algemene beskrywing van biometrika as “’n tegniek van persoonlike identifikasie wat gebaseer is op fisiese, fisiologiese of gedrags-karakterisering” is wyd genoeg om GGH in te sluit.

Voordat daar verder in besonderhede na biometrika in ons wetgewing gekyk word, is dit nodig om die groter regslandskap waarin GGH sal funksioneer, te beskryf. Die beginpunt in hierdie verband is die Grondwet van die Republiek van Suid-Afrika van 1996.

4.2 Die Grondwet van die Republiek van Suid-Afrika

Hoofstuk 2 van die Grondwet bevat ’n lys van regte wat alle mense in Suid-Afrika toekom.[66] In die konteks van GGH is minstens drie spesifieke menseregte van belang. Die eerste is die reg op gelykheid, wat in artikel 9 van die Grondwet vervat is. Subartikel (3) noem spesifiek dat die staat nie regstreeks of onregstreeks onbillik teen iemand mag diskrimineer nie. ’n Verskeidenheid spesifieke gronde word dan gelys, waaronder ras, geslagtelikheid, geslag, etniese herkoms en kleur. Daar is egter in beide die *Bridges*-beslissings genoem dat GGH-algoritmes opgestel word gegrond op databasisse van spesifieke etniese groepe, soos die reeds genoemde “white North European”[67] gesigte (in die *Bridges*-geval). Daar is egter nog geen instemmigheid in watter mate GGH-tegnologie teen rassegroepe “diskrimineer” nie, maar dit wil tog voorkom of die tegnologie steeds nie totaal diskriminasievry is nie.[68] In *R-Bridges* het die hof van appèl spesifiek genoem dat hierdie ’n saak is wat owerhede moet ondersoek voordat hulle GGH-sagteware in hul werksaamhede inspan.[69] Die etniese vooroordele van spesifieke sagteware moet getoets word alvorens dit in die veld in werking gestel word.[70] In Suid-Afrika is diskriminasie op grond van etnisiteit en kleur histories ’n baie sensitiewe kwessie,[71] en indien GGH hier ingespan sou word, sal owerhede baie versigtig moet trap om ’n stelsel te gebruik wat die mees etnies-neutrale resultate lewer.

Artikel 14 van die Grondwet bevat 'n tweede bepaling wat potensieel deur GGH tegnologie geskend kan word. Elkeen het die reg op privaatheid, en dit sluit onder andere in dat hul persoon, woning of eiendom nie deursoek mag word nie.[72] Met die eerste oogopslag kan dit voorkom of hierdie bepaling niks met GGH te doen het nie, maar dit is nie die geval nie. Artikel 8 van die Europese Konvensie vir Menseregte bevat 'n bepaling van 'n min of meer soortgelyke aard. Daar word genoem dat elkeen 'n reg het op respek vir hul private en gesinslewe, asook hul huis en kommunikasies. In *R-Bridges* het die hof van appèl spesifiek beslis dat hierdie bepaling verder strek as bloot 'n persoon se huislike lewe. Dit sluit ook 'n mate van privaatheid in die openbare sfeer in. Die hof het Britse uitsprake oor artikel 8 van die Europese Konvensie vir Menseregte in besonderhede gefynkam, en tot die slotsom gekom dat GGH inderdaad op 'n persoon se artikel 8-regte inbreuk maak, aangesien dit die sfeer van 'n persoon se identiteit in die openbaar binnedring.[73]

Daar kan natuurlik aangevoer word dat ten spyte daarvan dat artikel 8 van die Europese Konvensie vir Menseregte in wese met artikel 14 van die Grondwet ooreenstem, die Britse en Europese uitsprake nie by ons van toepassing is nie. Dit is natuurlik waar, maar aangesien daar geen presedent ten aansien van GGH in Suid-Afrika bestaan nie, sal 'n Suid-Afrikaanse hof nie ligtelik hierdie beslissings van die tafel vee nie. Dit wil dus voorkom of 'n GGH-ontplooiing deur die owerhede in Suid-Afrika tóg met hierdie bepaling van die Grondwet rekening sal moet hou.

GGH het die potensiaal om op 'n derde bepaling van die Grondwet inbreuk te maak, en dit is te vinde in artikel 17. Hierdie artikel noem dat elkeen die reg het om "vreedsaam en ongewapen te vergader, te betoog, 'n betooglinie te vorm en petisies voor te lê".[74] Dit is duidelik dat die wetgewer se oogmerk was dat daar uit vrye wil by so 'n betoging aangesluit kan word.[75] Indien GGH ingespan word om betogings te monitor, word intimidasie van owerheidsweë onmiddellik 'n faktor wat in aanmerking geneem sal moet word. Trouens, daar kan maklik aangevoer word dat GGH so 'n groot invloed op mense se optrede by betogings kan hê dat dit die aanwending van artikel 17 geheel en al in die wiele kan ry.[76]

4.3 Die Wet op Beskerming van Persoonlike Inligting 4 van 2013

Die Wet op Beskerming van Persoonlike Inligting (POPI-wet)[77] reguleer die insameling, berging en verdere verwerking[78] van persoonlike inligting. Dit is ook die wet wat die meeste toepassings vir GGH inhou.

4.3.1 Insameling

Wanneer die publiek se persoonlike inligting ingesamel word, vereis artikel 13 dat dit met 'n bepaalde oogmerk gedoen moet word. Die oogmerk moet duidelik en uitdruklik omskryf word,[79] en indien moontlik moet die datasubjek[80] van die insameling bewus wees.[81] Om hierdie bepaling in die konteks van GGH-tegnologie uit te voer, is oor die algemeen betreklik maklik.[82] In die *Bridges*-beslissing[83] het die Suid-Wallis-polisie hul GGH-stelsel vanuit gemerkte polisievoertuie ontplooi.[84] Hulle het selfs by verskeie geleenthede pamflette uitgegee om aan die publiek te verduidelik hoe die werking van die stelsel hulle sal raak.[85] Ten spyte van hierdie maatreëls om die publiek in te lig, blyk dit dat hierdie inligting nie wyd bekend was nie.[86] Bridges self het byvoorbeeld aan die hof genoem dat hy nie bewus was dat die GGH-stelsel ontplooi was totdat hy net etlike meter van die polisievoertuig was nie en die stelsel teen daardie tyd reeds sy gesigsbiometrika sou verwerk het.[87] Daar is dus geen sprake van verlening

van toestemming in so ’n geval nie. Uit hierdie gevallestudie blyk dit dat dit wél moontlik is om aan die vereiste dat die datasubjek van die insameling bewus moet wees, te voldoen, maar dat dit tog algemeen kan gebeur dat mense wie se biometriese inligting ingewin word, nie daarvan bewus sal wees nie.

Die belangrike aangeleentheid wat in die konteks van artikel 13 in gedagte gehou moet word, is dat enige persoon of owerheid wat GGH in Suid-Afrika wil uitrol, die spesifieke doel waarvoor dit beoog word, duidelik moet stel, en dat daadwerklike pogings aangewend sal moet om die datasubjek van die GGH in te lig. Daar word aan die hand gedoen dat die gebruik van die wetgewer in die Verenigde Koninkryk nagevolg kan word, waar ’n impakstudie, of ander verwante dokument, die doel van die GGH-stelsel uiteensit, en dieselfde dokument aandui watter stappe gedoen sal word om datasubjekte in te lig van GGH-stelsels wat hul biometriese inligting kan verwerk. In so ’n mate wys die GGH-operateur dat daar daadwerklike pogings aangewend is om aan artikel 13 te voldoen. Ten spyte daarvan dat toestemming nie verleen is nie, maak die POPI-wet voorsiening vir gevalle waar biometriese inligting sonder toestemming verwerk mag word.[88] Dit word hier onder bespreek,[89] maar in die konteks van artikel 13 moet daar in gedagte gehou word dat voordat ’n GGH-stelsel in Suid-Afrika ontplooi kan word, die oogmerk van die insameling van die inligting duidelik gestel moet word.

4.3.2 Berging

Artikel 14 van die POPI-wet bepaal dat rekords van persoonlike inligting nie vir ’n langer tydperk gehou moet word as wat noodsaaklik is nie. Dit is presies dieselfde beginsel as wat in artikel 39 van die Britse Data Protection Act 2018 vervat is.[90] In die *Bridges*-beslissings is daar groot gewag gemaak van hierdie beginsel, en veral waar GGH só ingespan word dat die verkreë gesigbiometrika dadelik uitgevee kan word as dit nie met die databasis van bekende verdagtes ooreenstem nie.[91] In so ’n geval word die publiek se regte in die grootste mate beskerm, aangesien die verkreë gesigsbiometrika nie later vir enige wetstoepassers beskikbaar is nie. Trouens, die oorgrote meerderheid van die verkreë gesigbiometrika kan nie eers deur enige mens beskou word nie, omdat dit so vinnig na verwerking uitgevee word.[92]

4.3.3 Verwerking

Die POPI-wet bevat ’n lywige definisie van *prosessering*[93] wat verwysing na verskeie toepaslike kwessies insluit. In die eerste plek word “outomatiese middele” van data-inwinning gemagtig, wat beteken dat die POPI-wet op enige GGH-sagteware van toepassing sal wees. Tweedens word enige vorm van persoonlike inligting by dié definisie ingesluit. In die derde plek word die metode van verwerking deeglik deur die wet beskryf, en val in drie kategorieë uiteen, te wete alle vorme van inwinning,[94] verspreiding[95] en verwerking[96] van data. Enige GGH-sagteware sal dus binne die definisie van *prosessering* val, aangesien dit baie wyd gedefinieer word.

Net soos die Britse Data Protection Act bevat die POPI-wet ook bepalings wat die verwerking van sensitiewe data verbied. Artikel 26 noem dit egter “spesiale persoonlike inligting”, en verduidelik dat dit “geloofs- of filosofiese oortuiginge, ras of etniese herkoms, vakbondlidmaatskap, politieke oortuiginge, gesondheid of sekslewe of biometriese inligting van ’n datasubjek” insluit.[97] Die “kriminele gedrag van ’n datasubjek” word ook as spesiale persoonlike inligting beskou. Enige verwerking van sulke data word spesifiek volgens artikel 26 verbied.[98] Dit is duidelik dat die verwerking van GGH-data binne die sfeer van spesiale persoonlike inligting val. Uit die *Bridges*-beslissing blyk dit dat gesigherkenningsagteware

potensieel bevooroordeeld teenoor ras, etnisiteit en geslag kan wees,[99] en dit val alles binne die sfeer van spesiale persoonlike inligting. Selfs algemene biometriese inligting word as deel van hierdie strenger kategorie beskou, en dit is duidelik dat enige verwerking van gesigbiometrika aan die strenger vereistes van artikel 26 sal moet voldoen.

Daar bestaan egter nie ’n algehele verbod op die verwerking van spesiale persoonlike inligting nie, aangesien artikel 27 ’n hele lys uitsonderings skep wat verwerking van sulke inligting magtig. Ongelukkig is hierdie lys so omvattend dat dit wil voorkom of daar nie ’n beduidend groot verskil bestaan tussen die verwerking van spesiale persoonlike inligting en “gewone” persoonlike inligting nie. Artikel 27(1)(b) magtig byvoorbeeld verwerking van spesiale persoonlike inligting indien dit noodsaaklik is om ’n reg of regsplig te beskerm. So ’n bepaling se trefwydte is egter ongelukkig so wyd dat dit in ’n magdom gevalle aanwending kan vind. Net so bepaal artikel 27(1)(d) dat verwerking van spesiale persoonlike inligting toelaatbaar is vir “historiese, statistiese en navorsingsoogmerke” indien dit in die openbare belang is,[100] of selfs indien dit onmoontlik sou wees of buitensporige moeite sou verg om toestemming tot sulke inligting te bekom.[101] Sodanige byna onbenullige uitsonderings op persoonlike dataverwerking hoort eintlik nie in ’n wet waar daar gepoog word om mense se privaatheid te beskerm nie. Die wetgewer noem darem dat voldoende waarborge voorsien moet word om die datasubjek nie buitensporig nadelig te beïnvloed nie, maar daar is geen bepaling in die wet wat noem aan wie die waarborg verskaf moet word nie. Daar word ook geen misdryf in hoofstuk 11 geskep wat die nakoming van artikel 27 reguleer nie. Daar word dan gewonder hoe effektief hierdie bepaling in die praktyk sal wees.

Aangesien die uitsonderings van artikel 27 so wyd is, wil dit voorkom of dit betreklik maklik sal wees om GGH-sagteware in ’n wetstoepassingskonteks, soos in die *Bridges*-saak gedoen is, te implementeer. Alhoewel spesiale persoonlike inligting verwerk word, sal die aanwending van GGH by wetstoepassing maklik onder die vaandel van “prosessering noodsaaklik … vir die vestiging, uitoefening of beskerming van ’n reg of regsplig” geplaas kan word.[102] Die regsbepaling is vaag genoeg om dit te magtig.

Die POPI-wet gaan egter nog veel verder deur wetstoepassers te magtig om persoonlike biometriese inligting te verwerk. Artikel 33(1) noem dat die bepalings van artikel 26 (die verbod op die verwerking van spesiale persoonlike inligting) glad nie op “liggame wat regtens belas is met die toepassing van die strafreg” van toepassing is nie. Asof dit nie genoeg is nie, bepaal dieselfde artikel dat “verantwoordelike partye wat daardie inligting regtens verkry het”, ook van artikel 26 vrygestel is. Dit beteken dat *enige* derde party wat deur wetstoepassers versoek of gemagtig word om inligting namens hul te verkry, dit mag doen sonder dat die verbod op die verwerking van spesiale persoonlike inligting op hulle van toepassing is. Dit is ’n drakoniese bepaling wat die potensiaal vir geweldige menseregteskendings inhou.

’n Praktiese voorbeeld sal hierdie punt illustreer. Sedert 2014 word optiese-vesel-internet in die stede van Suid-Afrika uitgerol. Saam met hierdie netwerk is ’n tweede netwerk van CCTV-videokameras, wat op bykans elke hoek in die stede van Suid-Afrika te vinde is, geskep.[103] Aangesien GGH-tegnologie ’n gewone CCTV-kamera as invoer kan gebruik, is dit reeds moontlik dat mense se optrede sonder hul medewete gemonitor kan word. Die maatskappy wat die videomateriaal deur hul kameranetwerk bekom, kan deur wetstoepassingsowerhede versoek of gemagtig word om GGH op die kameras te implementeer. Indien dit gedoen sou word, sou artikel 33(1) hierdie “verantwoordelike partye” kwytskeld van die vereistes van artikel 26.

Ongelukkig gaan die wet nóg verder deurdat artikel 33(3) wetstoepassingsowerhede magtig om biometriese inligting te bekom om hul inligting oor kriminele aktiwiteite aan te vul. Hierdie bepaling gaan eenvoudig te ver, aangesien dit in wese wetstoepassers in staat stel om *enige* inligting te bekom indien dit bloot onder die vaandel van "aanvulling" van inligting oor "kriminele gedrag" val. Dit is die teenoorgestelde benadering as wat in die *Bridges*-beslissings gevolg is.[104] In daardie beslissing is spesifiek genoem dat wetstoepassers se diskresie beperk moet word om menseregte te beskerm, maar die POPI-wet verskaf bykans geen beperkings op wetstoepassers se diskresie nie – indien die data-inwinning in enige opsig met die aanvulling van inligting oor kriminele gedrag te doen het, mag dit verwerk word.[105] Dit is ongetwyfeld die verkeerde benadering wat gevolg word, en sal nie veel help om menseregteskendings te verhoed nie. Die beslissing van *Vumacam v Johannesburg Road Agency*[106] wat hier onder bespreek word, deel hierdie sentiment, aangesien daar altyd 'n fyn balans behoort te wees tussen wetstoepassers se magte en die publiek se regte.

4.3.4 Geoutomatiseerde verwerking

In artikel 1 van die POPI-wet word *inligtingspasprogram* gedefinieer. Die Engelse weergawe van dieselfde wet noem dit 'n *information matching programme*, en dit behels eenvoudig enige sagteware wat 10 of meer datasubjekte van een databasis met 'n ander vergelyk.[107] Hierdie definisie pas GGH soos 'n handskoen, want dit is presies hoe GGH funksioneer – die sagteware skep 'n databasis met gesigherkenningskenmerke van bekende oortreders en verdagtes, soos die wetstoepasser dit bepaal, en hierdie bekende gesigherkenningskenmerke word met dié van nuwe gesigherkenningskenmerke, soos van die CCTV-videokamera verkry, vergelyk. Indien enige GGH-program in Suid-Afrika ingespan sou word, sal hierdie definisie ongetwyfeld daarop van toepassing wees, aangesien GGH die vermoë het om duisende gesigherkennings–kenmerke in 'n kort tydjie te verwerk en dit binne oomblikke na implementering meer as 10 datasubjekte, soos deur die wetgewing beperk, sal oorskry.

Indien enige inligtingspasprogramsagteware deur enigeen geskep word, moet die reguleerder[108] ondersoek instel of dit in die openbare belang is, en of die positiewe gevolge swaarder as die negatiewe gevolge weeg.[109] Daar moet ook bepaal word of daar nie ander, minder skadelike metodes is om dieselfde gevolg teweeg te bring nie.[110] Dit is baie interessante wetgewing hierdie wat nie 'n eweknie in die Britse Data Protection Act 2018 het nie. Indien enige verskaffer van GGH-sagteware só 'n stelsel in Suid-Afrika wil uitrol, sal die verskaffer hom aan ondersoek deur die reguleerder blootstel.

'n Verdere interessante aangeleentheid is dat die reguleerder volgens artikel 44(2)(e)(ii) moet bepaal of die inligtingspassing "uitermatig is" met inagneming van, onder andere, die hoeveelheid inligting wat gepas sal word. Dit is onseker hoe hierdie bepaling in die konteks van GGH geïnterpreteer sal word, want die inligting wat van die CCTV-kamera verkry word, word wel verwerk, maar die identiteit van die persoon word nooit bepaal voordat dit met 'n positiewe pasmaat in die databasis van verdagtes vergelyk word nie. Die kwessie van uitermatigheid kan dan vanuit twee hoeke beskou word: Enersyds kan daar aangevoer word dat GGH nie uitermatig is nie, want die hoeveelheid positiewe identifikasies sal nooit dié van die verdagte-databasis kan oorskry nie. Indien die databasis van verdagtes byvoorbeeld slegs 100 gesig-biometriese inligting bevat, sal die identifisering van individue nooit meer as 100 kan wees nie, selfs al word duisende gesigte van die CCTV-kamera verwerk. Die teenargument is dat die CCTV-beeldmateriaal honderde duisende *individuele* gesigte kan identifiseer, selfs al word die identiteit van die individu nie bepaal nie. In so 'n geval kan GGH maklik "uitermatig" wees.

In beide die *Bridges*-beslissings het die howe spesifiek daarop gewys dat dit een van die hoekstene van enige GGH-stelsel moet wees dat 'n veiligheidsmeganisme ingebou word wat 'n mens as die finale besluitnemer identifiseer.[111] Die stelsel wat die Suid-Wallis-polisie gebruik het, het aan hierdie vereiste voldoen.[112] Wanneer die GGH-stelsel 'n positiewe identifikasie gemaak het, het die sagteware een foto van die databasis en een foto van die verkreë CCTV-beeldmateriaal langs mekaar op 'n skerm vertoon. Dan kon die gebruiker sélf besluit of die twee foto's dié van dieselfde persoon is. 'n *Mens* het dus die finale besluit geneem.[113] Artikel 71 van die POPI-wet maak dit 'n spesifieke vereiste van enige inligtings–passisteem.[114] Enige GGH-sagteware wat dus nie aan hierdie vereiste voldoen nie, sal nie wettig in Suid-Afrika geïmplementeer mag word nie.

4.3.5 Gedragskodes

Artikel 60 van die POPI-wet maak voorsiening daarvoor dat die reguleerder gedragskodes kan uitreik wat op spesifieke situasies van toepassing is.[115] Dit beteken dat 'n gedragskode wat spesifiek die beginsels van GGH uiteensit, geskep kan word. Dit sal soortgelyk aan die Britse Surveillance Camera Code of Practice, of die Suid-Wallis Polisiedepartement se *Standard Operating Procedures* wees.[116] Sulke gedragskodes kan 'n betekenisvolle bydrae tot die reg lewer, mits dit korrek geformuleer word.

4.4 Die Wetsontwerp op Kubermisdade van 2017

In 2016 is die Wetsontwerp op Kubermisdade en Kubersekuriteit uitgevaardig.[117] Die wetsontwerp het gepoog om kubermisdade en -sekuriteit tot in die fynste besonderhede te reguleer. Dit wil voorkom of die wetgewer se ywer een te veel vir die Suid-Afrikaanse publiek was, omdat die wetsontwerp hewig gekritiseer is.[118] Die meeste kritiek was teen die kubersekuriteitdeel van die wetsontwerp gemik, en tereg. Die wetsontwerp het ingrypende magte ten aansien van die internet aan die staat oorgedra, en nadat wye negatiewe reaksie op die wetsontwerp ontvang is, het die wetgewer die deel van die wetsontwerp wat kubersekuriteit hanteer, verwyder.[119] Hierna is die wetsontwerp weer aangebied onder die vaandel van die Wetsontwerp op Kubermisdade.[120] Dit is baie meer gematig, en ten tye van hierdie bydrae is die wetsontwerp deur die Nasionale Raad van Provinsies aanvaar.[121] Dit lyk dus of die wet in die nabye toekoms in werking sal tree.

Artikel 45 van die wetsontwerp bepaal dat 'n polisiebeampte[122] enige data wat nie in die publieke sfeer is nie, regmatig mag ontvang indien die persoon wat die inligting in sy besit het, dit met toestemming aan die polisiebeampte beskikbaar stel.[123] In die konteks van GGH beteken dit dat 'n polisiebeampte hierdie bepaling sou kon gebruik om CCTV-videomateriaal te verkry wat byvoorbeeld deur straatvideokameras opgeneem is.[124] Indien die betrokke diensverskaffer gewillig is om die inligting beskikbaar te stel, kan dit regmatig deur wetstoepassers verkry word.[125] Artikel 45 temper die ontvangs van sulke inligting deur te bepaal dat dit onderhewig is aan "conditions regarding confidentiality and limitation of use". Indien die wetgewer hier geëindig het, sou dit ten minste die ontvangs van sulke inligting effens aan bande gelê het, maar die artikel lui verder "which he or she deems necessary". Die betrokke wetstoepasser word dus die *beoordelaar* van die ontvangs van sensitiewe inligting gemaak, en hy of sy mag besluit of die inligting verkry moet word. Dit is natuurlik die teenoorgestelde benadering van dié van die *R-Bridges*-appèlbeslissing. In daardie saak het die hof spesifiek genoem dat wetstoepassers se diskresie beperk moet word.[126] Deur dit te doen, word die publiek se regte

beskerm, veral gesien in die lig daarvan dat GGH van so 'n aard is dat dit op menseregte inbreuk kan maak sonder dat die slagoffer daarvan bewus is.

4.5 Vumacam v Johannesburg Road Agency

Die ongerapporteerde beslissing in *Vumacam v Johannesburg Road Agency*[127] illustreer die atmosfeer en sienings wanneer sensitiewe biometriese inligting ter sprake is. In wese het hierdie saak nie veel met GGH te doen nie, maar die groter aangeleentheid van verwerking van biometrika word hanteer. Die Johannesburgse Padagentskap (JRA) is verantwoordelik vir die uitreiking van reg-van-weg sertifikate (wayleaves in Engels).[128] Dit is dokumente wat privaat operateurs magtig om infrastruktuurontwikkelings rondom openbare paaie aan te bring. Vumacam het by verskeie geleenthede reg-van-weg sertifikate aangevra en dit is goedgekeur, aangesien Vumacam 'n erkende infrastruktuurontwikkelingsdiensverskaffer is. Sedert April 2019 het die JRA begin om Vumacam se aansoeke met omsigtigheid te hanteer, en dikwels af te keur.[129] Die hof[130] verklaar:

> JRA claims that Vumacam wants to install the cameras to surveil the movements of "innocent people" and sell the "footage" to third parties. [JRA] refers to the surveillance as "spy footage" which is a tradeable [sic] asset in the hands of Vumacam. The prevention and detection of crime is not the primary reason for the installation of the cameras, so alleges JRA. The essence of JRA's case is that Vumacam is spying on an individual's movements and thereby infringing on their rights to privacy.

Dit is dus duidelik dat die JRA verdere aansoeke van Vumacam afgekeur het omdat dit van mening is dat sensitiewe publieke inligting in die hande van 'n privaatoperateur beland, en daar geen maatreëls bestaan om daardie verskaffer te verhinder om die sensitiewe inligting na willekeur te gebruik nie.[131] Dit is baie interessant dat die JRA, soos die hof van appèl in *R-Bridges*, aangevoer het dat 'n regsraamwerk daargestel moet word alvorens sulke sensitiewe biometriese data ingewin en verwerk mag word.[132] Die hof meld:[133]

> To cope with the problems that arise from such spying activities a regulatory framework has to be established. The framework should focus on ensuring that the material collected through the cameras is handled in a manner that protects the privacy of individuals.

Om tot 'n korrekte bevinding te kom, ondersoek die hof die wetgewing wat op hierdie saak van toepassing is. Skedule 2 van die City of Johannesburg Metropolitan Municipality Public Road and Miscellaneous By-Laws[134] bevat die vereistes vir en proses wanneer reg-van-weg sertifikate toegestaan word.[135] Hierdie skedule maak dit duidelik dat indien dit blyk dat die diensverskaffer goedgekeur is vir werk rondom openbare paaie, en dit blyk dat die nodige prosedures bestaan om die infrastruktuur te beskerm, die magtigende owerheid die aansoek moet toestaan.[136] Nêrens in die wetgewing word daar enige melding gemaak dat die magtigende owerheid (in hierdie geval die JRA) 'n aansoek mag weier op grond van enige ander redes wat nie in skedule 2 vervat word nie. Die JRA is ten minste onder 'n verpligting om die aansoeke te oorweeg.[137] Gevolglik word die saak ten gunste van Vumacam beslis.[138]

Daar moet duidelik gemaak word dat Vumacam se oorwinning niks te doen het met die kwessie van potensiële privaatheidskending nie. Die hof noem byvoorbeeld dat die "lack of a legal framework, as mentioned above, is not a matter that falls within the purview of JRA. … [T]hat

issue – the legality or otherwise of the conduct – is not engaged here",[139] en beslis ook dat die kwessie van privaatheidskending "bears no relevance to the present case".[140] Die kern van dié saak was eerder die JRA se weiering om Vumacam se aansoeke vir reg-van-weg sertifikate te oorweeg. In daardie verband het die JRA gefouteer deur ander faktore in ag te neem as wat in skedule 2 van die magtigende wetgewing uitgestippel is.[141]

In hierdie saak is daar verskeie *obiter dicta* oor die verwerking van sensitiewe openbare inligting. Dit het selfs by name na GGH verwys.[142] Die belang van die saak is dat dit die algemene regsgevoel aangaande GGH en die verwerking van sensitiewe biometriese data illustreer. Een van die krities belangrike vereistes vir die suksesvolle implementering van GGH sonder om grootskaalse menseregteskendings te pleeg is 'n omvattende regsraamwerk wat individuele diskresie beperk en onnodige verwerking van sensitiewe data verbied.[143]

5. Slot

Dit is merkwaardig dat daar soveel raakpunte tussen Britse wetgewing en Suid-Afrikaanse wetgewing bestaan wanneer GGH beskou word. In Brittanje word die Europese Konvensie vir Menseregte as die basisdokument vir menseregte beskou, terwyl die Handves van Menseregte in die Suid-Afrikaanse Grondwet die ooreenstemmende beginsels uiteensit. Alhoewel artikel 8 van die Europese Konvensie vir Menseregte wyer as artikel 14 van die Grondwet geïnterpreteer word, blyk dit steeds dat dit nie baie van GGH-tegnologie sal verg om privaatheidskendings daar te stel nie. Daarom is dit belangrik dat daar 'n beperkende wetgewende raamwerk moet bestaan om sulke menseregtevergrype te reguleer. Die *Bridges*-beslissings het duidelik aangetoon hoe die Britse regsraamwerk ten aansien van GGH daar uitsien, en watter veranderinge aangebring behoort te word om dit meer menseregtevriendelik te maak. Omdat daar soveel raakpunte tussen wetgewing in die Verenigde Koninkryk en in Suid-Afrika bestaan, is dit nie vreemd dat aanbevelings in die *Bridges*-beslissings in 'n groot mate ook in Suid-Afrika behoort te geld nie.

Vervolgens word etlike wetgewende ingrepe vir Suid-Afrika voorgestel.

In die eerste plek kan gesigherkenningsdata as sensitiewe data ingevolge artikel 42 van die Data Protection Act 2018 beskou word. Dit word op dieselfde wyse in Suid-Afrika hanteer, waar artikel 26 van die POPI-wet bepaal hoe "spesiale persoonlike inligting" hanteer moet word. Die insameling en verwerking van sulke inligting moet aan streng vereistes voldoen, en die Suid-Afrikaanse stelsel bevat wél sulke bepalings, maar dit wil voorkom of die uitsonderings te wyd geformuleer is om op 'n sinvolle wyse menseregteskendings te verhoed. Verder verleen die Suid-Afrikaanse regsraamwerk te veel diskresie aan individuele operateurs in die privaat en publieke sfeer, wat die moontlikheid van menseregtevergrype vergroot. Daar word aan die hand gedoen dat uitsonderings in Suid-Afrikaanse wetgewing weer onder die loep geneem behoort te word om uitsonderings te verminder en te verfyn met die spesifieke doel om individuele diskresie te beperk.

Tweedens blyk dit dat gewone CCTV-beeldmateriaal as voedingsbron gebruik kan word om GGH-stelsels van data te voorsien. Die Britse Surveillance Camera Code of Practice bevat omvattende reëls waaraan CCTV-operateurs moet voldoen wanneer hulle sulke stelsels bedryf. Geen so 'n stelsel bestaan in Suid-Afrika nie, en daarom is dit nie vreemd dat die JRA in die

Vumacam v JRA-beslissing so bekommerd oor Vumacam se wye diskresie ten aansien van CCTV-tegnologie was nie. Hierdie bekommernis is nie ongegrond nie.[144] Gelukkig bevat die POPI-wet die moontlikheid dat gedragskodes uitgevaardig kan word wat aangeleenthede soos CCTV-stelsels en berging van die betrokke beeldmateriaal kan reguleer. Daar word ten sterkste aanbeveel dat so 'n gedragskode hier in Suid-Afrika uitgevaardig word, en die Britse Surveillance Camera Code of Practice kan 'n baie goeie basis as voorbeeld vorm.

In die derde plek blyk dit dat enige GGH-stelsel 'n *mens* as finale beoordelaar behoort te gebruik. Dit is iets waarop die *Bridges*-beslissings klem gelê het, en dit is gelukkig ook iets wat pertinent in Suid-Afrikaanse wetgewing aangespreek word. Hierdie kwessie behoort egter in meer besonderhede deur wetgewing gereguleer te word.

Vierdens behoort GGH-stelsels behoorlik getoets te word alvorens dit in die openbaar gebruik word. Suid-Afrika het 'n baie ryk etniese verskeidenheid, en die invloed van GGH-sagteware moet die moontlikheid van diskriminasie op grond van ras en etnisiteit soveel as moontlik beperk.

Dit blyk dat GGH-tegnologie sinvol in Suid-Afrika geïmplementeer kan word, mits die toepaslike regsraamwerk daarvoor behoorlik uitgebrei word soos hier bo aanbeveel is. Die basiese beginsels van so 'n stelsel is reeds in ons wetgewing te vinde, maar net soos in Brittanje is dit nog onvoldoende.

Aangesien hierdie tegnologie so 'n ingrypende invloed op menseregte kan hê, is dit belangrik dat ons wetgewer die nodige aandag daaraan gee sodat Suid-Afrikaanse burgers sinvol beskerm kan word.

Bibliografie

Amnesty International. 2020. Amnesty International calls for ban on the use of facial recognition technology for mass surveillance. https://www.amnesty.org/en/latest/research/2020/06/amnesty-international-calls-for-ban-on-the-use-of-facial-recognition-technology-for-mass-surveillance (16 September 2020 geraadpleeg).

Buolamwini, J.A. 2017. Gender shades: Intersectional phenotypic and demographic evaluation of face datasets and gender classifiers. PhD-proefskrif, Massachusetts Institute of Technology.

Burns, Y.M. 1997. Freedom of expression under the new Constitution. *Comparative and International Law Journal of Southern Africa*, 30(3):264–86.

Cliffe Dekker Hofmeyr. 2020. The Cybercrimes Bill is one step away from becoming law. https://www.cliffedekkerhofmeyr.com/en/news/publications/2020/technology/tmt-alert-7-july-The-Cybercrimes-Bill-is-one-step-away-from-becoming-law.html (2 Desember 2020 geraadpleeg).

Cybercrimes and Cybersecurity Bill 6 van 2017.

Cybercrimes Bill 6B van 2017. De Marsico, M. 2014. *Face recognition in adverse conditions.* Hershey Pennsilvanië: IGI Global.

Enerstvedt, O.M. 2017. *Aviation security, privacy, data protection and other human rights: Technologies and legal principles*. New York: Springer.

Gates, K.A. 2011. *Our biometric future: Facial recognition technology and the culture of surveillance*. New York: New York University Press.

Ho Hip, Chanté. 2020. Vumacam: Can they strike a balance between privacy and crime-fighting? *Sandton Chronicle*. https://sandtonchronicle.co.za/280102/what-is-your-expectation-of-privacy-2 (1 Oktober 2020 geraadpleeg).

Legislation.gov.uk. 2012. Protection of Freedoms Act 2012. https://www.legislation.gov.uk/ukpga/2012/9/section/29 (16 September 2020 geraadpleeg).

Li, H. en W. Guihua. 2019. Sample awareness-based personalized facial expression recognition. *Applied Intelligence*, 49(8):2956–69.

Li, S.Z. 2005. *Handbook of face recognition*. New York: Springer Science & Business Media.

Lowenberg, A.D. 1998. *The origins and demise of South African apartheid: A public choice analysis*. Ann Arbor Michigan: University of Michigan Press.

Mann, M. 2017. Automated facial recognition technology: Recent developments and approaches to oversight. *University of New South Wales Law Journal*, 40:121–45.

Marx, F.E. en N. O'Brien. 2011. To regulate or to over-regulate? Internet Service Provider liability: the industry representative body in terms of the ECT Act and regulations. *Obiter*, 32(3):537–56.

MIT Media Lab. 2018. Gender shades. https://www.youtube.com/watch?v=TWWsW1w-BVo (16 September 2020 geraadpleeg).

Modi, S.K. 2011. *Biometrics in identity management: Concepts to applications.* Londen: Artech House.

MyBroadband. 2015. New South African Cybercrimes bill is flawed. https://mybroadband.co.za/news/security/148477-new-south-african-cybercrimes-billis-flawed-r2k.html (16 September 2020 geraadpleeg).

Nkosi, T. 2019. Right to know raises concerns over Vumacam. https://ilovefourways.co.za/right-to-know-raises-concerns-over-vumacam (1 Oktober 2020 geraadpleeg).

Parlement van die Republiek van Suid-Afrika. 2020. NCOP passed the Cybercrimes bill, Civil Union and the Science and Technology Laws Amendment Bills. Persvrystelling, 1 Julie 2020. https://www.parliament.gov.za/press-releases/ncop-passed-cybercrimes-bill-civil-union-and-science-and-technology-laws-amendment-bills (16 September 2020 geraadpleeg).

Rocketreach. 2020. Vumatel information. https://rocketreach.co/vumatelprofile_b596dd9cf69fe201 (29 September 2020 geraadpleeg).

Schwenker, F. 2006. *Artificial neural networks in pattern recognition*. New York: Springer Science & Business Media.

Thornton, L. 2011. Costly to comply; even more if you don't. *Without Prejudice*, 11(2):63–4.

United Kingdom Home Office. 2013. Surveillance Camera Code of Practice. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf (9 September 2020 geraadpleeg).

Vumacam. 2020. www.vumacam.co.za. (30 September 2020 geraadpleeg).

Wong, C. 2018. We underestimate the threat of facial recognition technology at our peril. https://www.theguardian.com/commentisfree/2018/aug/17/we-underestimate-the-threat-of-facial-recognition-technology-at-our-peril (1 Oktober 2020 geraadpleeg).

Zhang, D. 2018. *Facial multi-characteristics and applications*. Singapoer: World Scientific.

Eindnotas

[1] Gates (2011:84); Li (2019:2956).

[2] Zhang (2018:17).

[3] 'n Voorbeeld van 'n GGH-stelsel in 'n wetstoepassingskonteks kan beskou word by *Edward Bridges v The Chief Constable of South Wales Police* (2019) EWHC 2341 (Admin) parr. 11–6.

[4] In *Bridges* par. 7 sê die hof: "Its use by public authorities also gives rise to significant civil liberties concerns." Sien ook Wong (2018) en Amnesty International (2020).

[5] Sien par. 4.3.3 vir 'n praktiese voorbeeld hiervan.

[6] Enerstvedt (2017:365).

[7] (2019) EWHC 2341 (Admin).

[8] (2020) EWCA Civ. 1058.

[9] *R-Bridges* par. 210 en Aanhangsel A tot die hofbeslissing.

[10] *Ibid*.

[11] *Bridges* par. 23; *R-Bridges* par. 8.

[12] De Marsico (2014:23) verduidelik dat "the faces are parameterized as triangulated meshes".

[13] Schwenker (2006:188).

[14] Li (2005:1).

[15] Modi (2011:73) beskryf dit so: "All individuals entering a certain area can be screened against a watch list with the aid of automated face recognition, and any probable hits can be passed onto human examiners for final determination." In *R-Bridges* par. 1 word die brondatabasis eweneens 'n *watchlist* genoem: "AFR Locate involves the deployment of surveillance cameras to capture digital images of members of the public, which are then processed and compared with digital images of persons on a watchlist compiled by SWP for the purpose of the deployment." (Interessant genoeg word daar oor die algemeen in Amerikaanse literatuur die skryfwyse *watch lists* gevind, terwyl dit in Britse literatuur gewoonlik *watchlists* is.)

[16] In Engels word daar algemeen na geslotebaantelevisie as CCTV (closed-circuit television) verwys. Die Engelse afkorting word so algemeen in Afrikaans gebruik dat daar besluit is om dit ook hier in verdere verwysings na hierdie tegnologie te gebruik. Dit word ook gedoen om algemene leesbaarheid van die teks te verbeter.

[17] *Bridges* par. 24(4).

[18] *Bridges* par. 33.

[19] In *R-Bridges* par. 187 word daar spesifiek genoem dat "[t]he identity of those who passed the camera without generating an alert is unknown."

[20] *Bridges* par. 37 en *R-Bridges* par. 17.

[21] *Ibid*.

[22] *Bridges* par. 7.

[23] *Bridges* parr. 11–16.

[24] *Bridges* par. 8.

[25] *Bridges* par. 159.

[26] *R-Bridges* parr. 209–10.

[27] *Bridges* par. 1 en *R-Bridges* par. 3.

[28] *Bridges* parr. 79–97 en *R-Bridges* parr. 54–202.

[29] *Bridges* par. 78 en *R-Bridges* par. 69.

[30] *Bridges* parr. 56–7.

[31] Afd. 1 van die konvensie bevat die handves van menseregte. Europese Konvensie vir Menseregte, 20 Maart 1952.

[32] *S v United Kingdom* (2009) 48 EHRR 50, 66; *Von Hannover v Germany* (2004) 40 EHRR 1, 50. Sien ook *Bridges* par. 47.

[33] 57. My beklemtoning.

[34] In die *Bridges*-saak parr. 62, 84 het die hof *a quo* beslis dat die eiser se art. 8-regte wel geskend was, maar dat die Suid-Wallis Polisiediens se optrede tóg binne die reg was. So ’n uitspraak mag dalk vreemd voorkom, maar die hof *a quo* het die werking van die GGH-stelsel van die Suid-Wallis Polisiediens in gedagte gehad. Daar is aan die hof verduidelik dat wanneer die stelsel geoutomatiseerde gesigherkenning uitvoer en dit blyk dat ’n persoon se gesigsdata nie met ’n voorafbepaalde databasis van verdagtes ooreenstem nie, dit sonder meer uitgevee word. Bridges was nooit op so ’n verdagtelys nie, en gevolglik sou sy gesigbiometrika slegs vir ’n oomblik binne die GGH-stelsel wees voordat dit uitgevee word (sien *Bridges* parr. 16, 37, 52). Die hof par. 84 het ook beslis dat die regsraamwerk waarbinne GGH toegepas word, nie ideaal is nie, maar tóg voldoende is om wettigheid te verseker.

[35] Sien par. 2 hier bo waar GGH-tegnologie bekendgestel word.

[36] Art. 29(1) van die Protection of Freedoms Act 2012.

[37] Die elektroniese weergawe van hierdie artikel is te vinde by Legislation.gov.uk (2012).

[38] Die kode is in 2013 uitgereik, en is te vinde by United Kingdom Home Office (2013).

[39] Die riglyne is die volgende:

“System operators should adopt the following 12 guiding principles:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date."

[40] Die Engelse woord wat hier gebruik word, is *surveillance*. Die Afrikaanse woord *waarneming* het 'n wyer, of meer algemene betekenis as die Engelse woord *surveillance*, maar in die konteks van hierdie bydrae blyk dit die beste beskrywing te wees.

[41] Riglyn 1.

[42] Riglyne 2 en 3.

[43] Riglyn 4 en 5.

[44] Riglyn 6.

[45] Riglyn 7 en 9.

[46] Riglyn 10.

[47] Die reguleerder t.a.v. hierdie dokument is die Surveillance Camera Commissioner. Sien art. 29(5)(e) van die Protection of Freedoms Act 2012.

[48] Art. 35(1).

[49] Art. 35(2)(a) en (b).

[50] Art. 35(4)(b).

[51] Art. 35(8)(b).

[52] Art. 42(2)(a).

[53] Art. 42(2)(b).

[54] Die artikel verskaf ook die minimum vereistes waaraan so 'n impakstudie moet voldoen:

"A data protection impact assessment must include the following—

(a) a general description of the envisaged processing operations;
(b) an assessment of the risks to the rights and freedoms of data subjects;
(c) the measures envisaged to address those risks;
(d) safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Part, taking into account the rights and legitimate interests of the data subjects and other persons concerned."

[55] Art. 149(1)(a) van die wet bepaal spesifiek dat alle publieke amptenare hul pligte so moet verrig dat "discrimination, harassment" en "victimization" in ag geneem moet word.

[56] *R (Brown) v Secretary of State for Work and Pensions* (2008) EWHC 3158 (Admin); (2009) PTSR 1506; *R (Hurley & Moore) v Secretary of State for Business, Innovation and Skills* (2012) EWHC 201 (Admin); (2012) HRLR 13.

[57] *Bridges* parr. 152–3 en *R-Bridges* parr. 164, 169.

[58] *R-Bridges* par. 189.

[59] *Bridges* par. 153 en *R-Bridges* parr. 196–8.

[60] Dit kan dus 'n wye groep mense insluit.

[61] Sien Buolamwini (2017). 'n Kort video wat hierdie interessante verskynsel verduidelik, kan besigtig word by MIT Media Lab (2018).

[62] Art. 44(2)(d) van die POPI-wet bepaal uitdruklik dat die reguleerder die werking van sagteware wat verwantskappe tussen verskillende databasisse onderneem, moet ondersoek vir korrekte werking.

[63] Die hof van appèl het Bridges op drie gronde gelyk gegee. Eerstens het die hof beslis dat die polisie se gebruik van GGH nie volgens die reg was nie, en dat art. 8 van die Europese Konvensie vir Menseregte oortree is. Gevolglik is Bridges se reg op privaat- en gesinslewe geskend. Tweedens is beslis dat die polisie se data-impakstudie nie aan die voorgeskrewe vereistes voldoen het nie, en derdens is beslis dat die polisie nie hul Public Sector Equality Duty ingevolge art .149 van die Equality Act nagekom het nie. Die uitspraak is gegee as 'n verklarende bevel (soos versoek deur die partye), en geen verdere remedies is toegestaan nie. *R-Bridges* par. 210.

[64] *R-Bridges* par. 210.

[65] Art. 1.

[66] Art. 7(1) verklaar: "Hierdie Handves van Regte is 'n hoeksteen van die demokrasie in Suid-Afrika. Dit verskans die regte van alle mense in ons land en bevestig die demokratiese waardes van menswaardigheid, gelykheid en vryheid."

[67] *R-Bridges* par. 189.

[68] Buolamwini (2017) asook MIT Media Lab (2018).

[69] *R-Bridges* par. 199.

[70] *Ibid*.

[71] Lowenberg (1998:56).

[72] Art. 14(a) en (b) van die Grondwet is hier saamgevoeg.

[73] *Bridges* par. 54. Let veral op die verwysing na *PG v United Kingdom (2008) 46*, waar daar genoem word dat wanneer 'n permanente rekord van publiekbeskikbare data van persone gestoor word, dit reeds art. 8 van die Europese Konvensie vir Menseregte skend.

[74] Sien ook Burns (1997:270–1).

[75] Burns noem spesifiek dat die reg op vergadering, betoging, linievorming en petisie 'n vorm van vryheid van uitdrukking is. Dit is dus duidelik dat enige vorm van owerheidsinmenging die regte in art. 17 sal ondergrawe.

[76] In die *Bridges*-beslissing het dit geblyk dat Edward Bridges tydens een geleentheid waar die GGH-stelsel ontplooi is, aan 'n vreedsame optog deelgeneem het. Indien betogers daarvan bewus word dat hul identiteit tydens sulke optogte aan polisiebeamptes bekend is (weens die gebruik van die GGH), kan dit hul gedrag verander en kan dit as intimidasie vanaf owerheidsweë gesien word.

[77] Die afkorting *POPI*, na aanleiding van die Engelse benaming van hierdie wet, is so algemeen in gebruik dat daar besluit is om hierdie akroniem te behou by die bespreking van die wet.

[78] Die wet praat deurgaans van "prosessering", maar ek verkies die Germaanse woord "verwerking", wat ek dus eerder sal gebruik, behalwe waar die wet aangehaal word.

[79] Art. 13(1).

[80] "Datasubjek" word deur die wet in art. 1 beskryf as "die persoon op wie persoonlike inligting betrekking het".

[81] Art. 13(2).

[82] Soms kan die geoutomatiseerde gesigherkenningstelsel totaal deursigtig wees, sodat die datasubjek nie eers van die monitering bewus is nie. Sien par. 4.3.3 vir 'n praktiese voorbeeld hiervan.

[83] Par. 11.

[84] *Ibid*.

[85] *Bridges* par. 39 en *R-Bridges* par. 19.

[86] *Bridges* par. 40.

[87] *Bridges* par. 12.

[88] Art. 27 van die POPI-wet.

[89] Afd. 4.3.3.

[90] Art. 39(1) van die Britse Data Protection Act 2018 bepaal: "The fifth data protection principle is that personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed."

[91] *R-Bridges* par. 17.

[92] *Ibid*.

[93] Sien eindnota 78 hier bo.

[94] Inwinning behels alle vorme van "insameling, ontvangs, optekening, organisering, insortering, stoor, opdatering of aanpassing, herwinning, aanpassing, konsultasie of gebruik".

[95] Verspreiding sluit prosesse soos "oorsending, verspreiding of beskikbaarstelling in enige ander vorm" in.

[96] Verwerking behels "samesmelting, koppeling, asook inperking, degradasie, uitwissing of vernietiging van inligting".

[97] Art. 26(a).

[98] Let egter daarop dat die verbod op die *verwerking* van sulke inligting slaan, en nie op die *inwin* daarvan nie. Trouens, die POPI-wet maak nêrens melding van die inwin van spesiale persoonlike inligting nie, maar slegs van die verwerking daarvan. Daar word aangeneem dat die inwin van spesiale persoonlike inligting deur die algemene beginsels van hfst. 3 van die POPI-wet gereguleer word. So 'n aanname blyk geregverdig te wees wanneer art. 4(3)(b) in gedagte gehou word waar daar terloops in die konteks van spesiale persoonlike inligting genoem word dat hoofstuk 3 se vereistes van toepassing is.

[99] *R-Bridges* par. 199.

[100] Art. 27(1)(d)(i).

[101] Art. 27(1)(d)(ii).

[102] Art. 27(1)(b).

[103] Vumacam (2020).

[104] Daar word aangevoer dat die *Bridges*-beslissing se benadering ongetwyfeld die korrekte een is, en dat die POPI-wet hier heeltemal te veel magte aan wetstoepassers verleen.

[105] Om aan wetstoepassers sulke vrye teuels te gee, kan verreikende gevolge inhou. 'n Goeie voorbeeld hiervan is die Australiese vervoerwetgewingstelsel. Mann (2017:125–6) verduidelik: "In late 2015 the *Road Transport Legislation Amendment (Release of Stored Photographs) Regulation 2015* (NSW) was introduced to amend clause 107 of the *Road Transport (Driver Licensing) Regulation 2008* (NSW). This permits the release of NSW Roads and Maritime Services ('RMS') photographs collected for the purpose of issuing driver licences to the NSW Crime Commission, the Australian Security Intelligence Organisation ('ASIO'), and the Identity Security Strike Team (Sydney), an inter-agency taskforce of the AFP and NSW Police. Under the amended clause 107, photographs may be released for the purposes of investigation of 'relevant criminal activity', a 'terrorist act' and 'threat of a terrorist act', or a 'terrorism offence'. It appears that images in the NSW RMS database can now be released without warrant or the knowledge or consent of individuals concerned."

[106] Afd. 4.5 hier onder.

[107] Die definisie van *inligtingspasprogram* lui so: "[D]ie vergelyking, hetsy fisies of by wyse van 'n elektroniese of ander instrument, van enige dokument wat persoonlike inligting van tien of meer datasubjekte bevat, met een of meerdere dokumente wat persoonlike inligting van tien of meer datasubjekte bevat vir doeleindes van die skep of kontrolering van inligting wat gebruik kan word vir die oogmerk om enige stappe in verband met 'n identifiseerbare datasubjek te doen."

[108] Die reguleerder waarna daar verwys word, is die inligtingsreguleerder ingevolge die POPI-wet. Hoofstuk 5 van die wet bevat die bepalings aangaande die instelling, bevoegdhede en werking van die reguleerder.

[109] Art. 44(2)(d).

[110] Art. 44(2)(e).

[111] *Bridges* par. 33.

[112] *Ibid*.

[113] *Ibid*.

[114] Art. 71 bepaal: "'n Datasubjek mag … nie onderhewig wees aan 'n besluit nie wat regsgevolge vir daardie datasubjek inhou, of wat daardie datasubjek op 'n wesenlike wyse raak, wat alleenlik geneem is op grond van die geoutomatiseerde prosessering van persoonlike inligting wat bedoel is om 'n profiel van sodanige persoon daar te stel …"

[115] Artikel 60(3) meld dat dit die reguleerder vry staan om gedragskodes volgens inligtingsoort, besigheidstipe, aktiwiteite of professie te skep.

[116] *Bridges* par. 41.

[117] Cybercrimes and Cybersecurity Bill (6:2017).

[118] Die webwerf MyBroadband (2015) noem bv.: "The new cybercrimes bill is flawed, too broad and brings the country one step closer to the securitisation of the internet." Sien ook Cliffe Dekker Hofmeyr (2020).

[119] *Ibid*.

[120] Cybercrimes Bill (6B:2017).

[121] Parlement van die Republiek van Suid-Afrika (2020).

[122] Art. 45 bevat ook die bewoording "sonder om spesifiek daartoe gemagtig te wees". Dit lyk of die wetgewer hier bepaal dat sulke inligting sonder 'n lasbrief verkry mag word.

[123] Dit is 'n eie vertaling van die betrokke artikel, aangesien die wetsontwerp tans slegs in Engels beskikbaar is. Die teks van die Engelse artikel lui soos volg:

"45. A police official may, without being specifically authorised thereto in terms of this Chapter, for the purposes of investigating any offence or suspected offence under Chapter 2 or section 17, 18 or 19 or any other offence or suspected offence in terms of the laws of the Republic which is or was committed by means of, or facilitated by the use of an article—

(a) receive, obtain or use publicly available data regardless of where the data is located geographically; or

(b) receive and use non-publicly available data, regardless of where the data is located geographically, if a person who is in control of, or possess the data, voluntarily and on such conditions regarding confidentiality and limitation of use which he or she deems necessary, discloses the data to a police official."

[124] In Suid-Afrika word optiese-vesel-internet sedert ongeveer 2014 uitgerol. Sien Rocketreach (2020). Die grootste optiese-vesel-diensverskaffer, Vumatel, het saam met sy veselnetwerk 'n verdere CCTV-videonetwerk ontwikkel. Oral waar optiese-vesel-kabels gelê is, is CCTV-kameras ook geplaas. Hierdie tweede netwerk staan bekend as Vumacam, en is 'n algemene gesig in Suid-Afrikaanse woonbuurte (sien Vumacam 2020).

[125] Dit kan dalk voorkom of hierdie stelling vergesog of spekulatief mag wees, maar ondervinding wys dat maatskappye dikwels ekstra moeite sal doen om goeie openbare betrekkings te bevorder en slegte publisiteit te vermy. Art. 77 van die Wet op Elektroniese Kommunikasies en Transaksies 25 van 2002 magtig internetdiensverskaffers om inligting binne hul beheer van die internet te verwyder indien hulle 'n afhaalkennisgewing ontvang. Oor die algemeen sal 'n internetdiensverskaffer sonder meer aan so 'n afhaalkennisgewing gehoor gee, ongeag of dit regverdigbaar is of nie. Dit is in die internetdiensverskaffer se eie

belang om die afhaalkennisgewing sonder enige beoordeling te gehoorsaam, aangesien dit die maklikste uitweg is, en art. 77(3) in elk geval bepaal dat ’n internetdiensverskaffer nie vir ’n onregmatige verwydering aanspreeklik gehou sal word nie (sien Marx 2011:542; Thornton 2011:64). Net so sal ’n internetdiensverskaffer eerder geneë wees om met wetstoepassers saam te werk sonder om te oordeel of so ’n versoek inderdaad regmatig is al dan nie.

[126] *R-Bridges* par. 55(2), 121–30. In hierdie paragrawe blyk dit duidelik dat die hof geensins beïndruk is met die wye diskresie wat polisiebeamptes kon uitoefen nie. Die hof (par. 130) noem bv. dat “the range is very broad and without apparent limits.”

[127] 2020-08-20. Saaknr. (HHSA).

[128] Par. 2. Die uitdrukking wayleave het glo sy oorsprong waar ’n grondeienaar ’n derde party “leave to cross the way” verleen. In die konteks van munisipale reg-van-weg sertifikate magtig dit spesifiek die derde party om die padoppervlak te breek of te beskadig om kabels, pype, of ander dienste-infrastruktuur te skep. Sien par. 4 van die beslissing.

[129] Par. 5.

[130] Parr. 6–7. Let daarop dat “[JRA]” hier in die aanhaling aangebring is. Die oorspronklike teks het “JVR” gehad, maar dit is ongetwyfeld ’n fout, aangesien daar in die hele beslissing slegs hierdie een keer van “JVR” melding gemaak word en dit ook nie na een van die regsgeleerdes of -firmas wat die saak hanteer het, kan verwys nie. Geeneen het hierdie voorletters nie.

[131] Par. 7.

[132] *Bridges* parr. 19, 63.

[133] *Ibid*.

[134] Ingevolge Kennisgewing 832 van Gauteng se *Provinsiale Koerant* gedateer 21 Mei 2004.

[135] Parr. 4, 12.

[136] Par. 13.

[137] Par. 13.

[138] Par. 20(3).

[139] Par. 17.

[140] Par. 18

[141] Par. 19.

[142] Par. 18.

[143] Par. 7.

[144] Sien ook *Sandton Chronicle* (2020).