WERKSMANS
ATTORNEYS

REGULATORY

POPIA and RICA – ACRONYMS AND PRIVACY

2 October 2019 *5 min read*

By Ahmore Burger-Smidt, Head of Data Privacy Practice

In digital era, privacy must be a priority. Is it just me, or is secret blanket surveillance obscenely outrageous?

– Al Gore

The right to privacy is a fundamental right afforded to all South African citizens in terms of the Constitution. The Protection of Personal Information Act, 2013 ("**POPIA**") gives credence to this right and brings with it responsibilities and duties that cannot be ignored.

The world around us is rapidly becoming a completely digitalised environment informed by technology. To this extent, disclosed or concealed personal information is an important aspect to consider, together with the extent of the minimum level of information required by businesses to conduct their operations.

On the one hand, there is a need for disclosure that is informed by multiple business requirements to achieve a variety of goals. These goals can be in the interest of the client, business or both parties. On the other hand, proper concealment is justified by the need to protect individual privacy. The growing use of digital devices has further complicated the dynamics between exposure or concealment and the obligation of businesses to protect the personal information of individuals *versus* the public interest when it comes to national security and the prevention, detection and prosecution of offences (amongst others).

There exists a need to understand the delicate legislative environment that companies operate in, within this digitalised technology driven environment.

The above requires consideration of certain crucial aspects in order for a balance to be found. The first aspect being a consideration of the leading purpose as to why personal information is required from and made available by an individual. The second is the relationships between individuals, business and public interest. The third is the proportionality of measures taken to reach the desired ends while considering individual privacy.

But on occasion, the dominating public interest determine to which extent disclosure of personal information is needed and compulsory. Public interest includes safety and security and could very well be privacy intrusive.

The Regulation of Interception of Communications and Provision of Communication-Related Information Act ("**RICA**") was passed in 2002 and came into effect in 2005. It regulates when government can surveil citizens through the interception of their communications. At the same time, its aim is to protect the privacy of communications, with exceptions, which are limited to serious crimes or threats to national security.

The constitutionality of RICA was challenged insofar as it permits the interception of communications of any person by any authorised state officials, subject to prescribed conditions. Under RICA, the state is allowed to tap telecommunications to detect any transnational threats. Judge Roland Sutherland ruled on Monday, 16 September 2019 that the practice of the State to implement "bulk interceptions" of telecommunications traffic in terms of RICA is unlawful.

The extent of mandatory exposure and concealment depends on the relationship between a data subject in the context of voluntary disclosure, which indicates the acceptance and acknowledgement of the dominant purposes and therefore the affiliated societal rights and duties, i.e. public interest. Thus, the right to demand information and the obligation to disclose must be defined according to the dominating purposes of a public interest and the related main involvement to achieve them.

However, proportionality of concealment and exposure in fulfilling dominating purposes is important. Any collection and processing of personal data should be proportionate, not exceeding necessity, unless with consent.

RICA requires telecommunications service providers to retain data for three years.

Judge Sutherland stated in this ruling "*In short, all of a person's personal telecommunications, up to three years past, lie in wait for the state to pry into, if its officials convince a judicial officer to authorise access*".[1]

Individuals should have an expectation (and thus a protection) of privacy, to the extent that personal information or data will not be used in ways that exceed necessity either by regulators or by other individual users and government. If such use is necessary, the use should be proportional to the desired ends and that means the choice of activities of the least harmful nature.

Digitalisation is a revolutionary stage in our society and brings with it fundamental changes that the still growing deployment of digital technologies will only enhance. It leads to challenges and affects our social life largely, and in ways never imagined to date. The crux of the fundamental changes lies in the created and increased information flow through various networks, which not only combines the physical space and the virtual one, but also adds new meanings to a hybrid of the two.[2] Escalating data collection, data processing, data storage, data dissemination and data retention have made the biggest threat to expose personal information to others, even to the rest of the whole world, in an unprecedented manner and thus they have generated numerous data privacy challenges, including, for instance, data misuse and abuse, function creep, stigmatisation and discrimination in individual life.

There is a growing demand for re-assuring the right to privacy expectation and privacy protection in all spheres of life, which could be fundamental and pre-conditional to the appropriate interpretation of public interest.

In view of these changes, the exploration of new boundaries and new balance between privacy protections, other desired values and public interest will continue. Nevertheless, one thing is quite certain, internalising privacy protection duties and obligations in the DNA of a business, is needed in view of its growing significance in the Digital Age.

---

[1] Amabhungane Centre for Investigative Journalism NPC & Another v Minister of Justice and Correctional Services & Others, Case No: 25978/2017

[2] M. Carmona "Contemporary Public Space: Critique and Classification, Part One: Critique" (2010) 15 Journal of Urban Design 126.



Ahmore Burger-Smidt

Head of Regulatory

View Profile