Ethics, citizenship and protecting human rights in the digital age

20 March 2019 – Fraud and identity theft; hacking; electronic vandalism; cyber terrorism and extortion; cyber stalking; invasion of privacy; cyber bullying and offensive material. These are just some of the digitally enabled crimes or illicit activities that can infringe on an individual's human rights. As we all start to become more active digital citizens, further consideration must be given to the protection of human rights to incorporate far more of the challenges faced in this digital age.

According to Pine Pienaar, Managing Director of Afiswitch; "Human rights differ from civil rights, in that this spectrum of rights are recognised as international standards for promoting and protecting an individual's basic right to a dignified human existence."

Pienaar explains that the idea is that all human rights are universal and unchallengeable within qualified legal boundaries; interdependent; equal and non-discriminatory – and, above all, the main duties to protect human rights falls on the governing states and their authorities or agents. "However, a number of the fundamental human rights that are potentially most at risk of being infringed on, or negatively affected, as a result of digitally enabled illicit acts include – the right to life, the rights to dignity and safety, and the right to personal privacy."

To put this into context;

Right to life:
Identity theft may not be directly responsible for the physical taking of a life, however, it can certainly impact the quality of life and even lead to devasting financial and/or legal implications for the unwitting victim. Global research notes that on average industries and consumers lose more than US$ 16 billion due to identity fraud every year.

With this in mind, Afiswitch believes that biometrics should form the foundation to any solution aimed at managing identity authentication and digital security. "The latest in biometrics solutions offer for more accurate identity verifications and are able to deliver results in real-time. This offers a real solution to 'knowing who you are dealing with' and can significantly assist in routing out fake personas and cybercriminals," says Pienaar.

Rights to dignity and safety
Pienaar indicates that beyond the potential of having one's dignity attacked, as a result of identity theft, cyberbullying is a growing worldwide phenomenon, which can be detrimental to an individual's mental and physical health – and it affects citizens of all ages, genders, race, cultures and religions or faiths.

A recent report showed that among 28 countries surveyed, South Africa had the highest prevalence of cyberbullying. In fact, 54% of parents who took part in the study admitted to knowing at least one child in their community who has been a victim of cyberbullying - up by 24% since 2011.

Riaan Badenhorst, General Manager of Kaspersky Lab Africa, says; "Although legal regulations across many markets are still developing, with the fast-moving world of social networking online, cyberbullying can cross over into cybercrime – and the personal effect of this should not be underestimated. All citizens should be protected from cyberbullying – and protecting a human's right to dignity, and safety, should extend to the online realm too."

Right to personal privacy

Pienaar suggests that this right is possibly most pervasively infringed on in the digital age. "Currently, the laws are evolving and trying to catch up with how much of a citizen's personal data is available online, but penultimately who the responsibility falls on to protect this data from breaches."

Lerato Thekiso, Founding Director: Thekvest Legal Advisory Services, agrees, but also suggests that with the efforts being undertaken by the State and international communities to protect the rights of citizens, careful consideration must also be given to the overarching authorisations of States and security communities to ensure that such authorisations do not infringe on the rights of citizens under the guise of national and international security.

"Such authorisation cannot be unrestricted as this opens the door for invasive surveillance, which, can infringe on a citizens' right to privacy. New laws and regulations around cybersecurity, protection of data and even biometric/identity-matching are aimed at addressing the challenges raised by new technologies and societal needs for new and added protection in what is becoming the 'new normal'. However, there needs to be a strong emphasis on ethical principles and behaviour to maintain trust. It will also become increasingly pivotal that sound ethics transcends through every sphere of government, business and citizens, if we are going to protect our sense of human society and citizenship in the evolving digital age," adds Thekiso.

Badenhorst states; "There needs to be wider acceptance that because we are functioning in a world continually shaped by technology and access to the Internet, then human rights protection must extend beyond the physical realm. And in support of this, more consideration must be given to how we employ IT security and online protection in the digital age – and to safeguard fundamental human rights and our right to be a protected digital citizen."

"It is also important to note that every citizen has the human right of responsibility too. This can be defined as having a duty to act in a way that still protects the rights and freedoms of other citizens – where no one citizen's actions should harm or infringe on the rights of another. This message seems to have been forgotten in our societal teachings of late but is certainly one that must be brought to the fore. We must teach our governments, our business sector and all corners of society what it means to be responsible digital citizens – and to always take care to protect the rights of others, on and offline," concludes Badenhorst.