Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: Elise Quevedo

The Dark Side of AI

From virtual assistants that manage our daily schedules to algorithms that predict our preferences, AI is embedded in our day-to-day, enhancing productivity and offering personalised experiences.

Even creating little cats and dogs that send you cute messages or fake AI digital partners may sound fun, right? But its potential for misuse can cast a shadow over its benefits because the capabilities that make AI advantageous and fun for personal and business use can also be weaponised, leading to scenarios where innocent fun morphs into malicious intent.

Trust me, the dark side of AI is real; I know this last part too well since I was at the receiving end of some fake and malicious trolling and bullying digitally not long ago. Luckily for me, this individual did it very poorly since they did not know enough about me (just professionally).

But what if this person knew more about me to make news that people would believe? This question is one of the reasons why, from a young age and since one of my first jobs at an internet cafe over two decades ago, I have been cautious about what I share online. One day, I may share the whole story about this trolling experience to teach others about resilience, what to do, and how to keep going if it happens to you.

From a young age, I saw how dangerous digital media can be when used for malice, so I have always preferred to keep most of my private life and friends to face-to-face, real-life interactions! But I was born into a generation without internet access or a mobile phone until I was a teenager. So, although I love technology, I am very aware of its dangers, and we don't speak often enough about it or how to protect ourselves.

Nowadays, children are born into a reality of oversharing; it has become the norm. Too many people share private and professional details without realising that this data can be used against them.

So, let's talk about the dark side of AI.

AI's Dual-Edged Sword

Deepfake technology, which uses AI to create hyper-realistic but fake audio and video content, has been employed to produce deceptive media that can tarnish reputations and disseminate false information. How many stories do you hear each month that involve deceptive media?

> Russian disinformation network used AI chatbots to spread pro-Kremlin propaganda

One example involves a Russian disinformation network that used AI chatbots to spread pro-Kremlin propaganda, sneaking into major AI platforms and twisting data processing to divulge false narratives. The realm of cybersecurity is not immune to AI's darker applications. My good friend, cybersecurity expert Ralph Echemendia, aka The Ethical Hacker, often says, "Nothing is ever 100% secure."

There have been situations where AI-generated deepfakes have been used to impersonate company executives, leading to fraudulent transactions and significant financial losses. This is not new; scammers have been doing it for a while. Back in 2019, they used AI-generated voices to impersonate the CEO of a UK-based energy firm, leading to the unauthorised transfer of $243,000.

AI Voice Cloning

Did you know that with just a few seconds of audio, as little as three to fifteen seconds, AI algorithms can accurately replicate a person's voice to the point you can't differentiate them? Imagine receiving a call from someone you know urgently needing financial assistance, only to realise that it was an AI-generated impersonation later on.

These scenarios are not hypothetical anymore. According to a study by McAfee, one in four individuals reported experiencing or knowing someone who had an AI voice-cloning scam, with 77% of those targeted losing money as a result.

There was a grandmother in Canada who received a call from what she believed was her grandson, claiming he had been in a car accident and needed bail money. In reality, scammers used AI to clone his voice from social media videos, deceiving her into wiring them thousands of dollars. This incident inspired the action-comedy movie Thelma.

> Have a keyword or sentence ready to use with those you trust that you can use in emergencies to make sure the person calling you is who they say they are

Many people regularly share voice or video recordings on social media, podcasts, and other platforms without considering the potential risks or implications. Cybercriminals quickly source these clips to create voice clones, making it a must that individuals be cautious about the content they share publicly.

You may have heard this before, but when it comes to money, have a keyword or sentence ready to use with those you trust (family/friends) that you can use in emergencies to make sure the person calling you is who they say they are. And if you have heard about this tip, have you implemented it?

Real-Life Implications

With AI-powered cloning technology becoming more sophisticated by the minute, cloning AI apps raises concerns over digital security and privacy because these apps allow users to manipulate images, videos, and voices without any technical knowledge. Most people use these applications for amusement, but others have abused them for malicious purposes, such as revenge porn and unapproved celebrity impersonation, which can have terrible emotional and psychological repercussions.

Deepfake technology has been employed in the political arena to create counterfeit videos of public figures, aiming to deceive and manipulate public opinion

Deepfake technology has also been employed in the political arena to create counterfeit videos of public figures, aiming to deceive and manipulate public opinion. Remember when a deepfake operation targeted US Senator Ben Cardin? AI-generated impersonations were used to extract sensitive political information. And how about the recent "Trump Gaza" AI video, which, although you can tell it is fake, went viral?

The increase of AI-generated explicit content, often referred to as "deepfake pornography," has unfortunately also emerged as a disturbing trend. Remember when it happened to Taylor Swift? The dark side of AI goes beyond celebrities and politicians. Recently, a network that distributed AI-generated images of child sexual abuse was taken down by police in 20 countries. If this fact is not worrisome and speeds up regulations, I don't know what will.

Challenging obstacles

Laws need to be created that discourage harmful use while encouraging innovation. When creating and applying AI, transparency can prevent abuse and guarantee that technology advances society without violating people's rights.

The negative aspects of AI serve as a reminder that while technology development and innovation have many advantages, they also present challenging obstacles. We can utilise AI responsibly if we remain informed, employ caution while interacting online, and support moral principles.

As we continue on this AI-driven future path, will we use this technology wisely or allow its darker potentials to overshadow its promise?