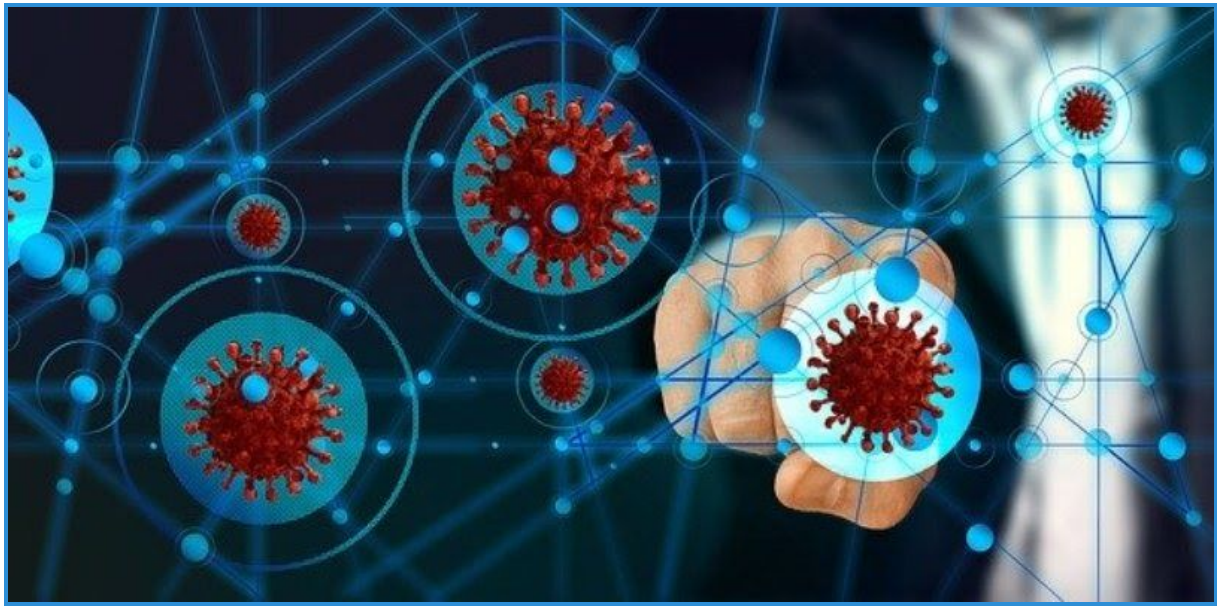# COVID-19 Pandemic and the Possibilities of Digital Surge

Post the COVID-19 pandemic scenario, there will be a tremendous surge in digital technologies and their usage, say IIM faculty

With the Covid-19 pandemic firmly settled in almost all countries of the world, a huge number of people locked down in homes are relying on digital means to talk, meet, work, argue, read about the world, express their concerns, and share their hopes. The digital networks are buzzing. Places like Bangalore are seeing an almost 100% rise in internet traffic.

At the same time, we see a rise in mischief-making, frauds, and scams. For instance, we have 'zoombombing' by mischief-makers who infiltrate Zoom sessions and hurl pornographic images at participants, usually during school and college online lectures. This has led many educational institutions around the world to ban Zoom conferences, and even the Indian government has issued warning notices.

A serious financial crime on the rise is fake sites collecting "relief" funds for the pandemic, pretending they are charitable organisations. Fake news of various kinds is also proliferating.

We anticipate that there will be a tremendous rise in digital technologies and their usage in the post-pandemic scenario. Along with this rise will come the risks, some of whose examples we have seen above. So what is one to do? Given the pervasiveness of technology and no easy way to shun it, do we have no option but to live with risks of technology use? We think not.

One way to address the risks associated with greater use of digital technologies is to understand the possibilities that technologies enable. These possibilities are also called affordances, which refers to the ways in which technology can be used. The manner of use is determined by immediate needs or may be determined by possibilities that become visible later.

Consider digital payments. Mobile wallets, UPI-based platforms, the PayTM wallet, are all examples of digital payments. They make life easier for us, as we can simply pay a merchant from our phone, without having to pull out our wallets and count cash, wondering if we have the change or the full amount. These are the readily visible possibilities.

The possibilities that are revealed as we begin to use the technology are: being able to see how we are spending our money, being able to estimate when and where to make most payments (or receive payments), and as we are seeing in COVID-19 times, making payments without any touch and hence reducing the chance of infection transmission.

On the other hand, the possibilities of mobile payments also encourage tricksters to engage in fraud. They see that people can be made to make payments remotely, so they find ways to lure them. One trick, common in India, is to ask people to reveal their debit card numbers and one-time-passwords by posing as bank managers. Another trick is to ask people for their account details to give them a refund, and then relieving them of thousands. Tricksters understand the sleight-of-hand possibilities of mobile payments, and prey on victims remotely.

Those who are unfamiliar with technology, do not understand its nuances and possibilities, are often scared of these hidden possibilities, as they appear like magic. Technology becomes an inscrutable and camouflaged threat, something to be wary of, to be touched, not embraced. We understand the roots of this anxiety and suggest the following, as the technology surge is inevitable, particularly after the pandemic recedes.

One, it is best to follow all suggested guidelines for security that are provided by any technology, be it Zoom or mobile wallets. This involves being aware of security issues that are known. Two, be aware of the security of related technologies – security of the smartphone, of the laptop, or the tablet – and ensure these guards are not lowered. A PayTM wallet, for instance, becomes insecure if the phone on which it resides is insecure. Three, explore the features and possibilities of each technology, what it can do and not do while using the technology. Research shows that younger people are likely to explore features more, as they spend more time with smartphones, than older people, who stick to doing what they know. Exploring features helps in knowing what is possible and what can be done. This also encourages users to take a critical look at the several opt-ins and opt-outs that the apps include.

It is also important for regulators, government and involved agencies and departments, to inform users about new technologies and their potential for use and misuse. For this purpose, we need to have dedicated think tanks and research groups who examine new

technologies with keen eyes to see the possibilities and the pitfalls. Lately, we have seen the Indian government being proactive on this front in the case of Zoom.

Of course, we understand that it is not always easy to visualize and estimate the ways in which technology will play out and affect our lives, which is why they are rightly termed as 'hidden' affordances. Many startups and now multi-billion dollar firms figured out some possibilities of technologies, before others, and created massively innovative companies – think of AirBnB and Uber – that had not existed before. The twin technologies of creating hash sequences and encryption, used for identifying and securing data, led to the development of Blockchains, whose possibilities were spotted by some firms that are now creating huge markets.

We also recognize that we may not see the possibilities even after many years of use. That fresh fruits, and the vitamins contained in them, could cure scurvy was known for over a hundred years before people recognised their potential and made them mandatory for sailors. In the technology domain, being vigilant of the possibilities of a solution, both positive and negative, may have significant implications for its further design and improvement. And, we believe, creators and users of technology have to play an equal role in ensuring their safe use, in a situation when we are no more left with an option to remain offline.

By:

Rahul De', professor of Information Systems, IIM Bangalore.

Neena Pandey, professor of Information Systems, IIM Visakhapatnam.

Abhipsa Pal, professor of Information Technology and Systems, IIM Kozhikode.