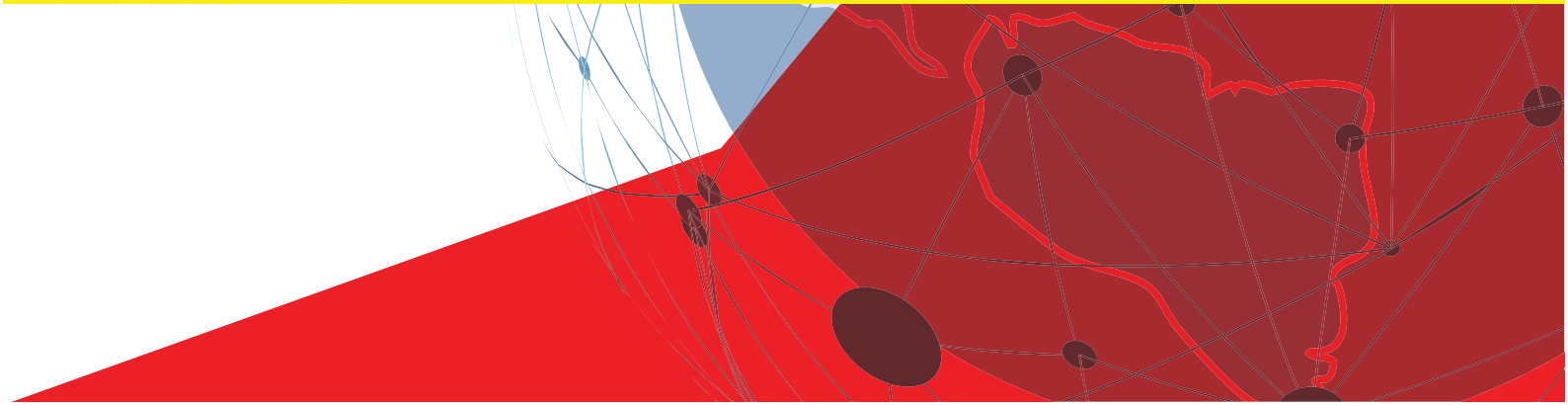
KTA ADVOCATES

AMANI IP NETWORK

Kampala | Dar es Salaam | **Nairobi**

legal ALERT

Coronavirus **COVID-19** , The Law & **4IR**



"The sapiens social order is imagined; humans cannot preserve the critical information for running it simply by making copies of their DNA. A conscious effort has to be made to sustain laws, customs, procedures and manner, otherwise the social order would quickly collapse" Prof. Yuval Noah Harari- Sapiens

The disruption to our imagined social order attributed to COVID-19 is unprecedented for at least 100 years. As the world grapples with continuity of even the simplest of services, such as grocery shopping, it would appear the fourth industrial revolution (4IR) is in unchartered territory.

This alert looks at the effect COVID will have on industry, specifically Technology, Media and Telecommunications; challenges and opportunities et al.

#staysafeworkfromhome

The Law, Cybersecurity and Data Protection

As companies and employers adopt remote working and social distancing, cybersecurity vigilance will become mandatory. The Electronic Transactions Act 2011(ETA), the Computer Misuse Act & the Electronic Signatures Act, 2011(ESA), lend credence to the success of the #STAYSAFEWORKFROMHOME initiative.

In Particular, The Electronic Transactions Act, 2011 essentially provides for the use, security, facilitation and regulation of electronic communications and online transactions. The Act (together with the Electronic Signatures Act, 2011) also significantly provides for the legal recognition of electronic transactions, records & signatures; which guarantees effective enforcement of the rights of consumers, if infringed.

Section 2 of the ESA, defines a digital signature as ***a transformation*** of a message using an ***asymmetric cryptosystem*** such that a person having the initial message and the signer's public key can accurately determine:

(a) whether the transformation was created using the private key that corresponds to the signer's public key; and

(b) whether the message has been altered since the transformation was made. In simple terms, a digital signature is a way to ensure that an electronic communication is authentic. By authentic we mean you know who is originating the electronic communication and you know the electronic communication has not been altered since it was made.

Section 2 of the ETA, defines an "advanced electronic signature" to mean an electronic signature, which is—

1. uniquely linked to the signatory;
2. reliably capable of identifying the signatory;
3. created using secure signature creation device that the signatory can maintain under his sole control; and
4. linked to the data to which it relates in such a manner that any subsequent change of the data or the connections between the data and signature are detectable.

Section 2 also defines an "automated transaction" to mean an electronic transaction conducted or performed, in whole or in part, by means of a data message in which the conduct or data messages of one or both parties is not reviewed by a natural person in the ordinary course of the natural person's business or employment.

Consequently, apart from the encumbrances of internet availability, connectivity and cost, it is possible to conclude almost any transaction online. Security will obviously be a major concern whilst communicating/transacting electronically. This will require utilizing platforms with strong encryption that will keep hackers, data miners and any other third party interference at bay.

Virtual Private Networks (VPN) may offer additional security if used correctly, supplemented by traditional methods such as password management, use of anti-viruses, spyware, firewalls among others. Furthermore, in the event of a security breach, containing the breach should be the first priority. In compliance with the breach notification law (discussed below), all breaches should be reported in order to minimize losses.

It is vital to keep in mind that with the stay at home campaign, cybercriminals are inadvertently on notice that every individual and business is fair game.

For most businesses in the 4IR, data is your most valuable resource. It is critical that all staff working from home appreciate Data Protection and Privacy laws such as the Uganda Data Protection and Privacy Act, 2019, the EU General Data Protection Regulation (GDPR) & the African Union Convention on Cyber Security and Personal Data Protection.

Data protection revolves around several principles encapsulated by notions that a data controller/processor should be accountable to the data subject for data collected, processed, held or used; data should be collected in a lawful and fair manner; it should be adequate, minimal and not excessive, accurate, not misleading & up to-date, collected transparently, shouldn't be kept longer than necessary, should be secure and overall should only be used for the purpose for which It is collected.

Section 20 of the 2019 act provides unequivocal guidelines for securing data, mandating data controllers to;

a) Identify reasonably foreseeable internal and external risks to personal data under that person's possession or control;

b) Establish and maintain appropriate safeguards against the identified risks;

c) Regularly verify that the safeguards are effectively implemented; and

d) Ensure that the safeguards are continually updated in response to new risks or deficiencies.

Additionally, under 22 (3) a data controller shall observe generally accepted information security practices and procedures, and specific industry or professional rules and regulations.

With the fluidity of the 4IR, industry practice in regards to safety while using Artificial intelligence (AI) and the Internet of Things (IOT) vigilance is king in ensuring best practice is observed. AI or Artificial Intelligence, Is technology that mimics human behavior. AI uses machine learning, where a computer program constantly perfects performing an assigned task by processing massive amounts of data and then identifying and analyzing new data more easily.

The Internet of Things (IoT) is the use of Intelligently connected devices and systems to harness data. This data is gathered by non-intrusive sensors and actuators in machines and other objects which, when connected to the Internet via Wi-Fi, Bluetooth and other networks aggregates data that can be used to improve all facets of life.

It is a well settled canon of law that an employer is vicariously liable for the acts of his employees. And, most often than none, it is the employees/contractors of a company that lose data even when state of the art security systems are in place.

It is thus imperative that organizations should follow the interpretative provisions set out in the UK data protection act 1998, Schedule 1, Pt II specifies that where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller should:

- choose an organization that offers guarantees about the security of the processing it is undertaking on the organization's behalf;
- put in place a written contract setting out the requirement for appropriate technical and organizational security measures and restricting processing to carrying out the data controller's instructions; and
- Take reasonable steps to ensure compliance with the security measures.

Section 23, of the 2019 act makes it mandatory for a data controller or processor who believes that personal data has been accessed or acquired by an unauthorized person to immediately notify the National Information Technology Authority (NITA). NITA will in turn determine if there's any need to notify the data subject(s).

The Cashless lockdown

COVID-19 has increased on the reliance/need for digital money and e-commerce. E- Commerce is in general parlance any activity that relates to the purchase and sale of goods and services over the Internet.

Studies have shown that Africa is the "mobile phone continent" of the world as more than half of the population owns a mobile phone. It was predicted that at the end of 2014 nearly 600 million Africans owned a mobile phone, and it's this mobile phone generation who are causing a surge in entrepreneurship. [1]

Uganda like the rest of the world, will rely on online banking, mobile money and by advertence e-Commerce platforms like Jumia, SafeBoda and Chap Chap that provide cashless solutions for online shopping if it is to reduce the physical exchange of fiat currencies.

Uganda currently lacks a comprehensive law for payment platforms. Pre-Covid-19, Parliament and Bank of Uganda had commenced public consultation on the National Payment System Bill, 2018 (NPS). The Bill is intended to regulate payment service providers and issuance of electronic money and to provide for safety and efficiency of payment systems.

The bill defines a payment system as a transaction through the transfer of monetary value, while a payment service means services enabling cash deposits or withdrawals and a Payment Service Provider is a person providing payment service.

1 https://www.virgin.com/entrepreneur/four-ways-mobile-phones-have-transformed-life-africa

Clause 5 of the Bill gives powers to the Central Bank to regulate, supervise and oversee operations of payment systems.

As Professor Yuval postulated, 'Every point in history is a crossroads. A single travelled road leads from the past to the present, but myriad paths fork into the future. Some of these paths are wider. Smoother and better marked, and are this more likely to be taken, but sometimes history or the people who make history- takes unexpected turns.....In a few decades, people will look back and think that the answers to all of these questions were obvious.'

It is not far-fetched to imagine that products like Safe Boda's Cashless will be key in a lockdown. For key sectors like transport and logistics, ride- hailing being a more organized industry, may be preferred and even wholly embraced by the different demographics; considering that in 2000 just one per cent of the African population owned a mobile phone and in 2014, 92 per cent of adult Tanzanians sent a least one text.

Consumer Protection

For e-commerce business, consumer protection will be key. The Electronic Transactions Act 2011, the Computer Misuse Act & the Electronic Signatures Act, 2011, provide for e-commerce and In particular, the Electronic Transactions Act, 2011 provides for the use, security, facilitation and regulation of electronic communications and online transactions.

The Act *(together with the Electronic Signatures Act, 2011)* also significantly provides for the legal recognition of electronic records & signatures; which guarantees effective enforcement of the rights of consumers, if infringed.

Sections 24-28 of the Electronic Transactions Act, 2011 make provision for consumer protection.

By law, every e-commerce entity must therefore:

- Provide to consumers via web site or through electronic communication where the goods or services are offered, details of ownership, physical and online address, details of membership to any self-regulatory or accreditation bodies, code of conduct to which that entity subscribes, registration number, names of directors and place of registration and importantly, the physical address where the person may be served with documents;

- Provide a description of the main characteristics of the goods or services offered by the person which is sufficient to enable a consumer to make an informed decision on the proposed electronic transaction;

- Indicate the full price of the goods or services, including transport costs, taxes and any other fees or costs including the manner of payment;
- Any terms or conditions of agreement, including any guarantees, that will apply to the transaction and how those terms may be accessed, stored and reproduced electronically by consumers;
- The time within which the goods will be dispatched or delivered or within which the services will be rendered;
- The manner and period within which consumers may access and maintain a full record of the transaction;
- The return, exchange and refund policy of the person;
- Any alternative dispute resolution code to which the person subscribes and how the code may be accessed electronically by the consumer;
- The security procedures and privacy policy of the person in respect of payment, payment information and personal information;
- Where appropriate, the minimum duration of the agreement in the case of agreements for the sale, hire, exchange or supply of products or services to be performed on an ongoing basis or recurrently;
- Provide a consumer with an opportunity to review the entire electronic transaction, correct any mistakes; and to withdraw from the transaction before placing an order;
- Provide options for cancellation with refunds of all payments made by the consumer after deducting the direct cost of returning the goods.

Financial services, including, investment services, insurance and reinsurance operations, banking services and securities are excluded from the above.

The provisions for cancellation do not apply in cases of supply of newspapers, periodicals, magazines and books, foodstuff, beverages or other goods intended for everyday consumption. This is if they are supplied to the home, residence or workplace of the consumer.

A customer is also estopped from cancelling where for audio/video recordings or computer software, the e-commerce entity is insulated against cancelation if the product is unsealed or if the goods supplied are personalized/made to the specifications of the consumer or by reason of their nature cannot be returned or are likely to deteriorate or expire.

Cancellation will also be impractical if the price for the supply of goods or services is dependent on fluctuations in the financial markets and which cannot be controlled by the supplier.

The ETA also prohibits sending unsolicited commercial communication to a consumer without consent or an opt out option.

Regulatory Sandboxes

Covid-19 will most likely also see the use of regulatory sandboxes to allow use of unregulated technology like drones and digital money. A regulatory sandbox is a framework set up by a regulator to allow small scale, live testing of innovations by private firms in a controlled environment (operating under a special exemption, allowance, or other limited, time-bound exception) under the regulator's supervision.

The National Payments Bill is Uganda's first (draft) legislation to provide for regulatory sandboxes for financial technology entities to live test their products.

The concept of regulatory sandboxes was developed in a time of rapid technological innovation and attempts to address the frictions between regulators desire to encourage and enable innovation and the emphasis on regulation.

Regulatory sandboxes are being applied in Africa's financial sector to foster innovation. In May, 2019, Kenya's Capital Markets Authority approved the, Regulatory Sandbox Policy Guidance Note that allows Digital Finance Services (DFS) players to deploy and conduct live-tests of their innovative products, solutions, and service for a maximum period of 12 months.

Earlier in 2018, Sierra Leone in collaboration with United Nations Capital Development Fund (UNCDF) and Financial Sector Deepening Africa (FSDA), introduced a regulatory sandbox framework, The Sierra Leone FinTech Initiative. South Africa also plans to set up its Fintech Hub and sandbox in the first half of 2020.

Regulatory sandboxes will be key if government considers the possibility of utilizing unmanned propulsion systems (drones) either for relief purposes, transport or even e-commerce.

Drones have in the past few year, gained notoriety as a cheaper, more efficient mode of transport. In the less developed world where the transport ecosystem is in most cases worse for wear, drones have been deployed to deliver medicines, blood and life-saving supplies to hard to reach areas.

In 2019, the Ugandan government approved, as safe for use, medical drones procured by Infectious Disease Institute (IDI) to deliver essential medical supplies to hard-to-reach places. The project by IDI will see 'medical drones' deliver the first batch of ARVs in March, 2020 to Kalangala District, an island usually only accessible by boats and ferry[2]. Another organization, Uganda Flying Labs, deploys drones for mapping and data analytics.

In 2016, UNICEF and the Government of Malawi, piloted a drone project for early detection of HIV in infants. The project is an apt African drone success story as it reduced the time for delivery of blood samples from 11 days to less than 30 minutes; from rural clinics to testing laboratories.[3]

Tanzania's drone-based mapping project of Zanzibar, in collaboration with the World Bank, enabled open sharing of collected data with local communities and has since helped promote innovative approaches for data usage in disaster management[4].

Regulatory sandboxes may be key in lawfully deploying drones to combat Covid-19. The United Kingdom's Civil Aviation Authority recently launched an innovation sandbox to work with seven companies working on particular drone related projects, including Amazon's prime Air.[5]

---

nomic Forum, Drone Innovators Network Summit, India, October, 2019.

4 http://www3.weforum.org/docs/WEF_Advanced_Drone_Operations_Toolkit.pdf

5 https://www.caa.co.uk/Our-work/Innovation/The-CAA-regulatory-sandbox/

Recommendations

In order to safely implement #STAYATHOMEWORKFROMHOME, organizations should:

- Put in place data protection and data privacy policies and review their existing policies through a data audit. A data audit shall be able revisit these and ensure compliance. Alongside this, it is important to pay attention to overseas data transfers and that the countries to which your business is exporting data have similar data protection and privacy laws to Uganda so that your customers' data is at all times kept safe within the confines of data protection laws.
- Come up with or review remote work policies and therein include data protection and cyber security provisions. A work at home arrangement, should be well thought out and the employees should be provided with guidance notes; your company should make provisions for split site availability, a well-established agile working program, remote access to data, data recovery and remote IT support for telecommuters.
- Organizational security controls must be in place concerning the organization's software among others.
- Ensure that companies' internal legal teams and Data Protection Officers are vigilant and work closely with the IT teams so that operations remain legally compliant even though the day to day way of running the business has changed drastically.
- Provide training so as to raise the workforce's awareness around key issues, such COVID-19 specific cybersecurity threats such as phishing emails, fraudulent websites and malicious apps, any changes in any policies as a result of COVI-19, guidance on the use and access of sensitive data over untrusted Wi-Fi networks.
- The use of trusted sources, such as the Uganda government sanctioned, https://covid19.gou.go.ug website for up-to-date, fact-based information on COVID-19.
- Training may be required for members who are not used to working from home, the kind of roles that they will need to perform among others. With this, it is vital to remember to remain compliant with the Employment laws of Uganda as provided for under the Employment Act, 2006 and the Employment Regulations, 2011 to govern your employer- employee relationships. Employment contracts are in most, if not all cases, very specific, so your company's human resource should be alive to the rights of employees and all the legal issues that manifest during this period.
- We advise on the implementation of measures such as document encryption, frequent change of passwords, tracking and having control of who has access to your company's technology and methodology, also you have to secure networks to prevent a data breach during this time.
- For contract renegotiation, ensure you have adequate data protection clauses.
- Every business should also put in place data protection, data privacy, data retention and data destruction policies in line with the Data Protection and Privacy Act, 2019 of Uganda.

https://www.monitor.co.ug/News/National/Drones-delivering-medical-supplies-ICT-exhibition-Kalangala/688334-5392086-12lg76e/index.html Details of the UNICEF drone project were provided by Jaime Archuleda, the UNICEF Global Lead for Drones at the World Economic Forum, Drone Innovators Network Summit, India, October, 2019. http://www3.weforum.org/docs/WEF_Advanced_Drone_Operations_Toolkit.pdf

https://www.caa.co.uk/Our-work/Innovation/The-CAA-regulatory-sandbox/

TMT TEAM

Kenneth Muhangi
Managing Partner

Grace Eron Nanyonjo
Associate

Ivan Allan Ojakol
Associate

Judith Babirye Kagere
Junior Associate

HELP
STOP THE
SPREAD
AND STAY HEALTHY

We end with a call to action for all Ugandans, #STAYHOMESTAYSAFE.

FLoor 3,
Plot 4, Hannington Road
P.O. Box 37366, Kampala, Uganda.

T +256 414 530 114
F +256 414 531 078
E partners@ktaadvocates.com